VES-1124

24-port QAM 2-band VDSL Switch

User's Guide

October 2004

Version 3.50(LP.0)

ZyXEL

Unleash Networking Power

Copyright

Copyright © 2004 by ZyXEL Communications Corporation

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patents rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Interference Statements and Warnings

FCC

Interference Statement:

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning!

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策.

Certifications

Refer to the product page at www.zyxel.com.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Customer Support

If you have questions about your ZyXEL product or desire assistance, contact ZyXEL Communications Corporation offices worldwide, in one of the following ways:

Contacting Customer Support

When you contact your customer support representative, have the following information ready:

- Product model and serial number.
- Firmware version information.
- Warranty information.
- Date you received your product.
- Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[1] FAX[1]	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

[1] "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

Copyright ..... **ii**

Interference Statements and Warnings ..... **iii**

ZyXEL Limited Warranty ..... **iv**

Customer Support ..... **v**

Table of Contents ..... **vi**

List of Figures ..... **x**

List of Tables ..... **xiii**

Preface ..... **xv**

Chapter 1 Getting to know the VES **1-1**

1.1 Overview 1-1

1.2 Features1 1-1

1.3 Applications 1-4

Chapter 2 Hardware Connections **2-1**

2.1 Front Panel 2-1

2.2 Front Panel LEDs 2-2

2.3 Rear Panel 2-3

Chapter 3 Introducing the Web Configurator **3-1**

3.1 Introduction 3-1

3.2 System Login 3-1

3.3 Status Screen 3-1

3.4 Switch Lockout 3-6

3.5 Resetting the Switch 3-6

Chapter 4 Status, Port Details and VDSL Summary **4-1**

4.1 Overview 4-1

4.2 Port Status 4-1

Chapter 5 Basic Setting **5-1**

5.1 Introducing The Basic Setting Screens 5-1

5.2 System Information 5-1

5.3 General Setup 5-4

5.4 Introduction to VLANs 5-5

5.5 IGMP Snooping 5-6

5.6 Switch Setup Screen 5-6

5.7 IP Setup 5-9

5.8 Port Setup 5-10

5.9 VDSL Parameters 5-13

5.10 VDSL Common Setup 5-14

5.11 VDSL Profile Setup 5-14

5.12 Viewing and Editing VDSL Profiles 5-16

Chapter 6 VLAN 6-1
6.1 Introduction to IEEE 802.1Q Tagged VLAN 6-1
6.2 802.1Q VLAN 6-3
6.3 Introduction to Port-based VLANs 6-10

Chapter 7 Static MAC Forward Setup 7-1
7.1 Introduction to Static MAC Forward Setup 7-1
7.2 Configuring Static MAC Forwarding 7-1
7.3 Viewing and Editing Static MAC Forwarding Rules 7-2

Chapter 8 Spanning Tree Protocol 8-1
8.1 Introduction to Spanning Tree Protocol (STP) 8-1
8.2 STP Terminology 8-1
8.3 How STP Works 8-1
8.4 STP Status 8-2

Chapter 9 Bandwidth Control 9-1
9.1 Introduction to Bandwidth Control 9-1

Chapter 10 Broadcast Storm Control 10-1
10.1 Introducing Broadcast Storm Control 10-1
10.2 Configuring Broadcast Storm Control 10-1

Chapter 11 Mirroring 11-1
11.1 Introduction to Port Mirroring 11-1
11.2 Port Mirroring Configuration 11-1

Chapter 12 Link Aggregation 12-1
12.1 Introduction to Link Aggregation 12-1
12.2 Link Aggregation Protocol Status 12-2
12.3 Link Aggregation Setup 12-3

Chapter 13 Port Authentication 13-1
13.1 Introduction to Authentication 13-1
13.2 Configuring Port Authentication 13-1

Chapter 14 Port Security 14-1
14.1 About Port Security 14-1
14.2 Port Security Setup 14-1

Chapter 15 Access Control 15-1
15.1 About Access Control 15-1
15.2 Access Control Overview 15-1
15.3 About SNMP 15-2
15.4 Service Access Control 15-6
15.5 Remote Management 15-6

Chapter 16 Queuing Method 16-1
16.1 Introduction to Queuing 16-1
16.2 Configuring Queuing 16-1
16.3 Weighted Round Robin Scheduling Example 16-2

Chapter 17 Routing Protocol 17-1
17.1 Static Route 17-1

Chapter 18 Maintenance 18-1
18.1 Maintenance 18-1
18.2 Firmware Upgrade 18-1
18.3 Restore a Configuration File 18-2
18.4 Backing Up a Configuration File 18-2
18.5 Load Factory Defaults 18-3
18.6 Reboot System 18-4
18.7 Command Line FTP 18-4

Chapter 19 Diagnostic 19-1
19.1 Diagnostic 19-1

Chapter 20 Cluster Management 20-1
20.1 Introduction to Cluster Management 20-1
20.2 Cluster Management Status 20-2
20.3 Configuring Cluster Management 20-4

Chapter 21 MAC Table 21-1
21.1 Introduction to MAC Table 21-1
21.2 Viewing MAC Table 21-2

Chapter 22 ARP Table 22-1
22.1 Introduction to ARP Table 22-1
22.2 Viewing ARP Table 22-1

Chapter 23 Introduction to CLI 23-1
23.1 Command Line Interface Overview 23-1
23.2 Command Summary 23-2

Chapter 24 Command Examples 24-1
24.1 Commonly Used Commands Overview 24-1
24.2 sys Commands 24-1
24.3 sys cluster Commands 24-3
24.4 ip Commands 24-5
24.5 vdsl Commands 24-6
24.6 Enabling rstp on a VDSL Port 24-8

Chapter 25 IEEE 802.1Q Tagged VLAN Commands 25-1
25.1 IEEE 802.1Q Tagged VLAN Overview 25-1
25.2 Filtering Databases 25-1
25.3 Configuring Tagged VLAN 25-2
25.4 IEEE VLAN1Q Tagged VLAN Configuration Commands 25-3
25.5 vlan1q svlan active 25-8
25.6 vlan1q svlan inactive 25-8
25.7 vlan1q svlan list 25-8

Appendix A Troubleshooting ..... A

Appendix B Pin Assignments ..... A

Appendix C Product Specifications ..... E

Index I

List of Figures

Figure 1-1 MTU Application 1-4
Figure 1-2 Curbside Application 1-5
Figure 2-1 VES-1124 Front Panel 2-1
Figure 2-2 VES-1124 Back Panel 2-3
Figure 3-1 Web Configurator: login 3-1
Figure 3-2 Web Configurator Status Screen 3-2
Figure 3-3 Web Configurator: Change Password at Login 3-6
Figure 3-4 Resetting the VES Via Command 3-7
Figure 3-5 Uploading the Default Configuration File Via Console Port 3-8
Figure 3-6 Web Configurator: Logout Screen 3-8
Figure 4-1 Status 4-2
Figure 4-2 Status: VDSL Summary 4-4
Figure 4-3 Status: VDSL Port Details 4-5
Figure 4-4 Status: Port Details (Ethernet) 4-9
Figure 5-1 System Info 5-2
Figure 5-2 General Setup 5-4
Figure 5-3 Switch Setup 5-7
Figure 5-4 Port Setup 5-11
Figure 5-5 VDSL Common Setup 5-14
Figure 5-6 VDSL Profile Setup 5-15
Figure 5-7 VDSL Profile Setup: Summary Table 5-16
Figure 6-1 Selecting a VLAN Type 6-3
Figure 6-2 802.1Q VLAN Status 6-3
Figure 6-3 802.1Q VLAN Port Settings 6-5
Figure 6-4 802.1Q Static VLAN 6-7
Figure 6-5 Static VLAN: Summary Table 6-8
Figure 6-6 VID1 Example Screen 6-9
Figure 6-7 Port Based VLAN Setup (All Connected) 6-11
Figure 6-8 Port Based VLAN Setup (Port Isolation) 6-12
Figure 7-1 Static MAC Forwarding 7-1
Figure 7-2 Static MAC Forwarding: Summary Table 7-2
Figure 8-1 Spanning Tree Protocol: Status 8-3
Figure 8-2 Spanning Tree Protocol: Configuration 8-5
Figure 9-1 Bandwidth Control 9-1
Figure 10-1 Broadcast Storm Control 10-1
Figure 11-1 Mirroring 11-2
Figure 12-1 Aggregation ID 12-2
Figure 12-2 Link Aggregation: Link Aggregation Protocol Status 12-2

Figure 12-3 Link Aggregation: Configuration 12-3
Figure 13-1 RADIUS Server 13-1
Figure 13-2 Port Authentication 13-2
Figure 13-3 Port Authentication: RADIUS 13-2
Figure 13-4 Port Authentication: 802.1x 13-3
Figure 14-1 Port Security 14-2
Figure 15-1 Access Control 15-1
Figure 15-2 Console Port Priority 15-1
Figure 15-3 SNMP Management Model 15-2
Figure 15-4 Access Control: SNMP 15-4
Figure 15-5 Access Control: Logins 15-5
Figure 15-6 Access Control: Service Access Control 15-6
Figure 15-7 Access Control: Remote Management 15-7
Figure 16-1 Queuing Method 16-2
Figure 16-2 Weighted Round Robin Scheduling Configuration Example 16-3
Figure 16-3 Weighted Round Robin Scheduling Ratio Example 16-3
Figure 17-1 Static Routing 17-1
Figure 17-2 Static Routing: Summary Table 17-2
Figure 18-1 Maintenance 18-1
Figure 18-2 Firmware Upgrade 18-2
Figure 18-3 Restore Configuration 18-2
Figure 18-4 Backup Configuration 18-3
Figure 18-5 Confirm Load factory Defaults 18-3
Figure 18-6 Restart Switch After Load Factory Defaults 18-3
Figure 18-7 Confirm Restart the Switch 18-4
Figure 19-1 Diagnostic 19-1
Figure 20-1 Clustering Application Example 20-1
Figure 20-2 Cluster Management Status 20-2
Figure 20-3 Cluster Member Web Configuration Screen Example 20-3
Figure 20-4 Example: Uploading Firmware to a Cluster Member Switch 20-4
Figure 20-5 Configuring Cluster Management 20-5
Figure 21-1 MAC Table Filtering Flowchart 21-1
Figure 21-2 MAC Table 21-2
Figure 22-1 ARP Table 22-1
Figure 23-1 CLI Help: Sample Output 23-2
Figure 24-1 sys log disp Command Example 24-1
Figure 24-2 sys version Command Example 24-2
Figure 24-3 sys sw vlan1q vlan list Command Example 24-2
Figure 24-4 sys sw pktcnt Command Example 24-3
Figure 24-5 sys sw mac list Command Example 24-3

Figure 24-6 sys cluster status Command Example 24-4
Figure 24-7 sys cluster showMember Command Example 24-4
Figure 24-8 sys cluster status Command Example 24-5
Figure 24-9 IP PING Command Example 24-5
Figure 24-10 ip route status Command Example 24-6
Figure 24-11 ip arp status Command Example 24-6
Figure 24-12 ip dhcp Command Examples 24-6
Figure 24-13 vdsl profile list Command Example 24-7
Figure 24-14 vdsl profile apply Command Example 24-7
Figure 24-15 vdsl port status display Command Example 24-8
Figure 24-16 vdsl setmode Command Example 24-8
Figure 25-1 Tagged VLAN Configuration and Activation Example 25-2
Figure 25-2 CPU VLAN Configuration and Activation Example 25-2
Figure 25-3 Deleting Default VLAN Example 25-3
Figure 25-4 GARP STATUS Command Example 25-3
Figure 25-5 garp timer Command Example 25-4
Figure 25-6 garp status Command Example 25-4
Figure 25-7 vlan1q port status Command Example 25-5
Figure 25-8 vlan1q port default vid Command Example 25-5
Figure 25-9 vlan1q port accept Command Example 25-6
Figure 25-10 vlan1q port gvrp Command Example 25-6
Figure 25-11 vlan1q svlan cpu Command Example 25-6
Figure 25-12 Modifying the Static VLAN Example 25-7
Figure 25-13 vlan1q svlan delentry Command Example 25-8
Figure 25-14 vlan1q svlan list Command Example 25-9
Figure 25-15 vlan1q status Command Example 25-9

List of Tables

Table 2-1 VES-1124: Front Panel 2-1
Table 2-2 LED Descriptions 2-2
Table 3-1 Navigation Panel Sub-links Overview 3-3
Table 3-2 Web Configurator Screens Overview 3-3
Table 3-3 Navigation Panel Sub-link Descriptions 3-4
Table 4-1 Status 4-3
Table 4-2 Status: VDSL Port Details 4-6
Table 4-3 Status: Port Details (Ethernet) 4-10
Table 5-1 System Info 5-2
Table 5-2 General Setup 5-4
Table 5-3 Switch Setup 5-7
Table 5-4 IP Setup 5-9
Table 5-5 Port Setup 5-12
Table 5-6 VDSL Common Setup 5-14
Table 5-7 VDSL Profile Setup 5-16
Table 5-8 VDSL Profile Setup: Summary Table 5-17
Table 6-1 GARP Terminology 6-2
Table 6-2 802.1Q VLAN Status 6-3
Table 6-3 802.1Q VLAN Port Settings 6-6
Table 6-4 802.1Q Static VLAN 6-8
Table 6-5 Static VLAN: Summary Table 6-8
Table 6-6 Port Based VLAN Setup 6-12
Table 7-1 Static MAC Forwarding 7-1
Table 7-2 Static MAC Forwarding: Summary Table 7-2
Table 8-1 STP Path Costs 8-1
Table 8-2 STP Port States 8-2
Table 8-3 Spanning Tree Protocol: Status 8-3
Table 8-4 Spanning Tree Protocol: Configuration 8-6
Table 9-1 Bandwidth Control 9-2
Table 10-1 Broadcast Storm Control 10-1
Table 11-1 Mirroring 11-3
Table 12-1 Link Aggregation: Link Aggregation Protocol Status 12-3
Table 12-2 Link Aggregation: Configuration 12-3
Table 13-1 Port Authentication: RADIUS 13-2
Table 13-2 Port Authentication: 802.1x 13-4
Table 14-1 Port Security 14-2
Table 15-1 Access Control Summary 15-1
Table 15-2 SNMP Commands 15-2

Table 15-3 SNMP Traps 15-3
Table 15-4 Access Control: SNMP 15-4
Table 15-5 Access Control: Logins 15-5
Table 15-6 Access Control: Service Access Control 15-6
Table 15-7 Access Control: Remote Management 15-7
Table 16-1 Queuing Method 16-2
Table 17-1 Static Routing 17-1
Table 17-2 Static Routing: Summary Table 17-2
Table 18-1 Filename Conventions 18-4
Table 18-2 General Commands for GUI-based FTP Clients 18-5
Table 19-1 Diagnostic 19-1
Table 20-1 ZyXEL Clustering Management Specifications 20-1
Table 20-2 Cluster Management Status 20-2
Table 20-3 FTP Upload to Cluster member Example 20-4
Table 20-4 Configuring Cluster Management 20-5
Table 21-1 MAC Table 21-2
Table 22-1 ARP Table 22-2
Table 23-1 Command Summary: sys 23-2
Table 23-2 Command Summary: sys sw 23-6
Table 23-3 Command Summary: exit 23-11
Table 23-4 Command Summary: ip 23-12
Table 23-5 Command Summary: vdsl 23-13
Table 23-6 Command Summary: config 23-15
Table 23-1 Troubleshooting Data Transmission ..... A
Table 23-2 Troubleshooting a Non-Constant VDSL LED ..... B
Table 23-3 Troubleshooting the SYNC-rate ..... B
Table 23-4 Troubleshooting the VES's Configured Settings ..... B
Table 23-5 Troubleshooting the Password ..... B
Table 23-6 Troubleshooting a Remote Server C
Table 23-7 Troubleshooting Connecting to the Switch C

Preface

About this User's Manual

This user's guide gives hardware specifications and explains web configurator and command line configuration, management, and troubleshooting for the switch.

Online Registration

Register your ZyXEL product online at www.zyxel.com for free future product updates and information.

General Syntax Conventions

- Mouse action sequences are denoted using a comma. For example, click **Start, Settings, Control Panel, Network** means first you click **Start**, click or move the mouse pointer over **Settings**, then click or move the mouse pointer over **Control Panel** and finally click (or double-click) **Network**.
- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- Predefined choices are in **Bold Arial** font.
- Button and field labels, links and screen names in are in **Bold Times New Roman** font.
- A single keystroke is in Arial font and enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- For brevity's sake, we will use "e.g.," as shorthand for "for instance", and "i.e.," for "that is" or "in other words".

Naming Conventions

- The VES-1124 24-port QAM 2-band VDSL Switch may be referred to as the VES-1124, the VES, the switch or, simply, as the device.
- This user's guide refers an Ethernet device as a switch in general for feature background information.

Related Documentation

- Web Configurator Online Help

Embedded web help for descriptions of individual screens and supplementary information.

- Glossary and ZyXEL Web Site

Please refer to www.zyxel.com for an online glossary of networking terms or the ZyXEL download library for additional support documentation.

Part I:

Getting Ready

This part acquaints you with the features and applications of the VES-1124, instructs you how to make the hardware connections, understand the front panel LEDs.

Chapter 1
Getting to know the VES

This chapter describes the key features, benefits and applications of the VES-1124.

1.1 Overview

The VES-1124 is a stand-alone layer-2 VDSL over Ethernet switch with two Telco-50 connector port for 24 VDSL and 24 POTS/ISDN connections. The VES-1124 also comes with two 10/100Base-TX uplink ports.

With its built-in web configurator, managing and configuring the switch is easy. From cabinet management to port-level control and monitoring, you can visually configure and manage your network via the web browser. Just click your mouse instead of typing cryptic command strings. In addition, the switch can also be managed via Telnet, the console port, or third-party SNMP management

1.2 Features1

The next two sections describe the hardware and firmware features of the VES.

1.2.1 Hardware Features

QAM Modulation

The VES, combined with the Prestige 841 VDSL modem, provides service providers a QAM (quadrature amplitude modulation)-based VDSL solution.

Band Plan Support

The VES supports various VDSL band plans (ETSI, ANSI/ETSI and 10 BaseS).

Two Telco-50 Connection Ports

There are two Telco-50 connectors for 24 VDSL and POTS/ISDN connections respectively.

10/100 Mbps Fast Ethernet Ports

The two Ethernet ports allow you to aggregate the ports into one logical link. This provides the opportunity for a faster network connection.

They allow for the VES to connect to:

- A second level switch

- Daisy-chain to other switches

Integrated Splitters

The integrated DSL/ISDN splitter eliminates the need to use external splitters that separate the voice-band and DSL signals.

Console Port

Use the console port for local management of the switch.

Fans

The fans cool the VES sufficiently to allow reliable operation of the switch in even poorly ventilated rooms or basements.

1.2.2 Firmware Features

IP Protocols

- IP Host (No routing)
- Telnet for configuration and monitoring
- SNMP for management
  - SNMP MIB II (RFC 1213)
  - SNMP v1 RFC 1157
  - SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP
  - Ethernet MIBs RFC 1643
  - Bridge MIBs (RFC 1493, 2674)
  - SMI RFC 1155
  - RMON MIB (RFC 1757 Group 1, 2, 3, 9)
  - VDSL private MIB

Management

- Web configurator
- Command-line interface locally via console port or remotely via Telnet
- SNMP

System Monitoring

- System status (link status, rates, statistics counters)
- SNMP
- Temperatures, voltage, fan speed reports and alarms
- Port Mirroring allows you to analyze one port's traffic from another.

Security

- System management password protection
- IEEE 802.1Q VLAN
- Limit dynamic port MAC address learning
- Port-based VLAN
- 802.1x Authentication
- Static MAC address filtering

Port Link Aggregation

The VES adheres to the 802.3ad standard for static and dynamic port trunking.

Bandwidth Control

The VES supports rate limiting in 64Kbps increments allowing you to create different service plans

The VES supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your switch.

Broadcast storm control

Quality of Service

Two priority queues so you can ensure mission-critical data gets delivered on time.

Follows the IEEE 802.1p priority setting standard.

STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

IGMP Snooping

With IGMP snooping, group multicast traffic is only forwarded to ports that are members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

Cluster Management

Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

1.3 Applications

These are the main applications for the VES:

- Internet access and multimedia services for Multiple Tenant Units (MTU).
- Other applications include telemedicine, surveillance systems, remote servers systems, cellular base stations and high-quality teleconferencing.

1.3.1 MTU Application

The following diagram depicts a typical application of the VES with Prestige 841 VDSL modems, in a large residential building, or multiple tenant unit (MTU), that leverages existing phone line wiring to provide Internet access to all tenants. Note that VDSL service can coexist with voice service on the same line.

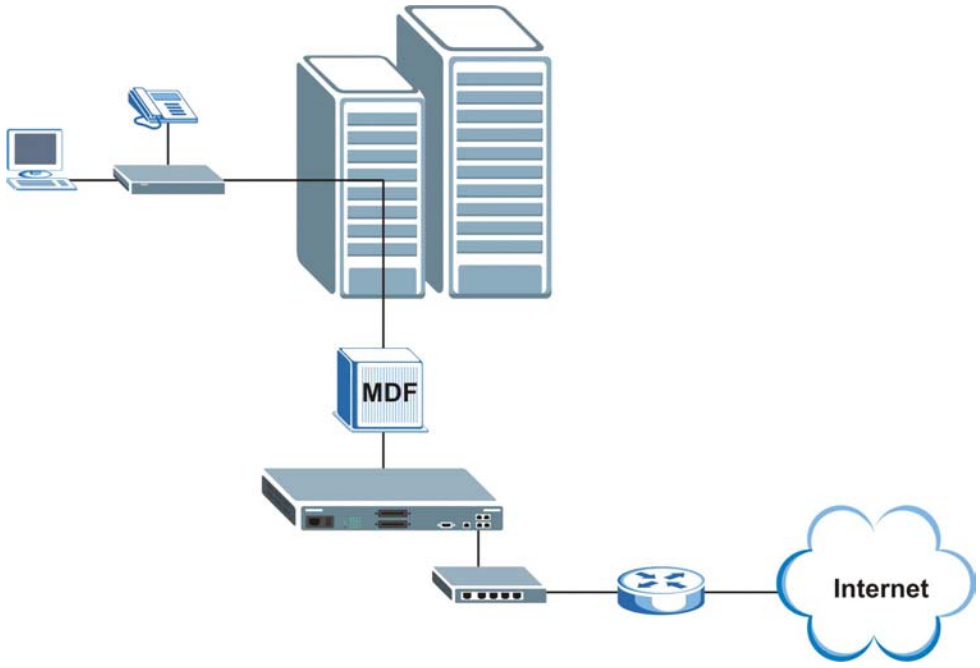


Figure 1-1 MTU Application

1.3.2 Curbside Application

The VES can also be used by an Internet Service Provider (ISP) in a street cabinet to form a "mini POP (Point-of-Presence)" to provide broadband services to residential areas that are too far away from the ISP to avail of DSL services. Residents need a VDSL modem, for example the Prestige 841, connected as shown in the previous figure.

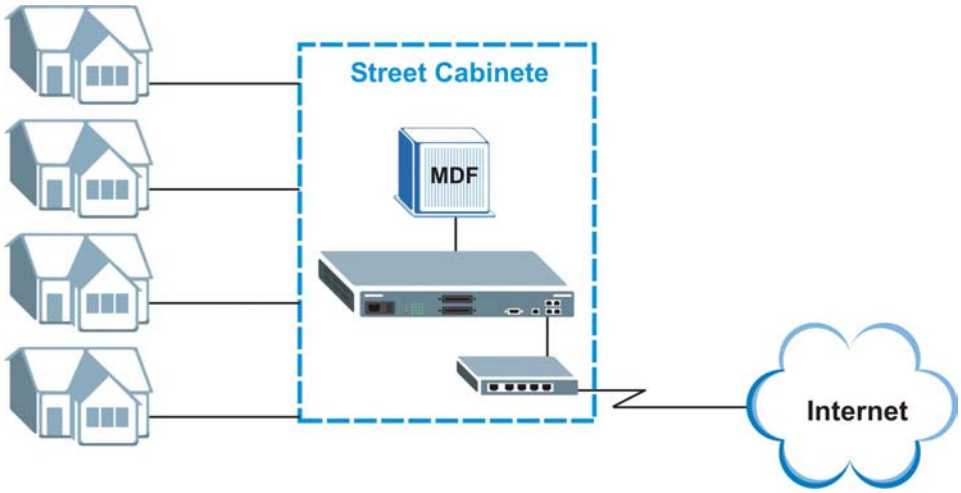


Figure 1-2 Curbside Application

Chapter 2
Hardware Connections

This chapter acquaints you with the front and rear panels, shows you how to make the connections and install/remove optional modules.

2.1 Front Panel

The following figure shows the front panel of the VES-1124. The front panel contains switch LEDs, two Telco-50 connectors and a console port for local switch management and two uplink ports.

Figure 2-1 VES-1124 Front Panel

The following table describes the ports on the front panel.

Table 2-1 VES-1124: Front Panel

CONNECTOR	DESCRIPTION
CONSOLE	The CONSOLE port is an RS-232 port for local configuration of the VES-1124.
CO	The CO Telco-50 port connects to the central office or a PBX.
USER	The USER Telco-50 port connects to the user (subscriber) VDSL equipment.
10/100 (25, 26)	These uplink ports allow you to connect to any switch.

2.1.1 Console Port Connection

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the VES. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

2.1.2 VDSL Port Connections

Connect the lines from the user equipment (VDSL modems) to the **USER** port and the lines from the central office switch or PBX (Private Branch Exchange) to the **CO** port. Make sure that the **USER** line and the **CO** lines are not shorted on the MDF (Main Distribution Frame).

The line from the user carries both the VDSL and the voice signals. For each line, the VES has a built-in splitter that separates the high frequency VDSL signal from the voice band signal and feeds the VDSL signal to the VES, while the voice band signal is diverted to the CO port.

See the appendix for details on the Telco-50 connector pin assignments

2.1.3 10/100M Auto-Sensing Ethernet

The VES has 10/100Mbps auto-sensing Ethernet ports. There are two factors related to Ethernet: speed and duplex mode. In 10/100Mbps Fast Ethernet, the speed can be 10Mbps or 100Mbps and the duplex mode can be half duplex or full duplex. The auto-negotiation capability makes one Ethernet port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.

When auto-negotiation is turned on, an Ethernet port on the VES negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the VES determines the connection speed by detecting the signal on the cable and using half duplex mode. When the VES's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

You may also bundle the two Ethernet ports into one logical 200Mbps link.

Default Settings

The factory default settings for the Ethernet ports of the VES are:

- Speed: Auto
- Duplex: Auto
- Flow control: Enable
- Trunking: Disabled

Use a straight through Ethernet cable when connecting the VES to an Ethernet switch. Use a crossover Ethernet cable if you are daisy-chaining multiple VESes and make sure trunking is disabled.

2.2 Front Panel LEDs

The following table describes the LED indicators on the front panel of the VES-1124.

Table 2-2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/malfunctioning.

Table 2-2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
VDSL (1~24)	Green	On	The link to the VDSL modem is up.
		Off	The link to the VDSL modem is down.
10/100 (25, 26)	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		On	The link to a 10 Mbps Ethernet network is up.
		Off	The link to a 10 Mbps Ethernet network is down.
	Yellow	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to a 100 Mbps Ethernet network is down.

2.3 Rear Panel

The following figure shows the rear panel of the VES. The rear panel contains the power receptacle and the power switch.

For continued protection against risk of fire, replace only with same type and rating of fuse.
AC INPUT
100-240VAC 50/60Hz 1A MAX
FUSE T3A250VAC

Figure 2-2 VES-1124 Back Panel

2.3.1 Power Connector

Make sure you are using the correct power source.

To connect the VES, plug the female end of the power cord to the power receptacle on the rear panel. Connect the other end of the cord to a power outlet. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

Part II:

Web Configurator Getting Started

This part introduces you to the VES web configurator including accessing and navigating, a screens overview and how to configure the **Basic Setting** screens.

Chapter 3
Introducing the Web Configurator

This section introduces the configuration and functions of the web configurator.

3.1 Introduction

The embedded web configurator allows you to manage the switch from anywhere through a standard browser such as Microsoft Internet Explorer or Netscape Navigator.

Use Internet Explorer 5.5 and later or Netscape Navigator 6 and later versions.

3.2 System Login

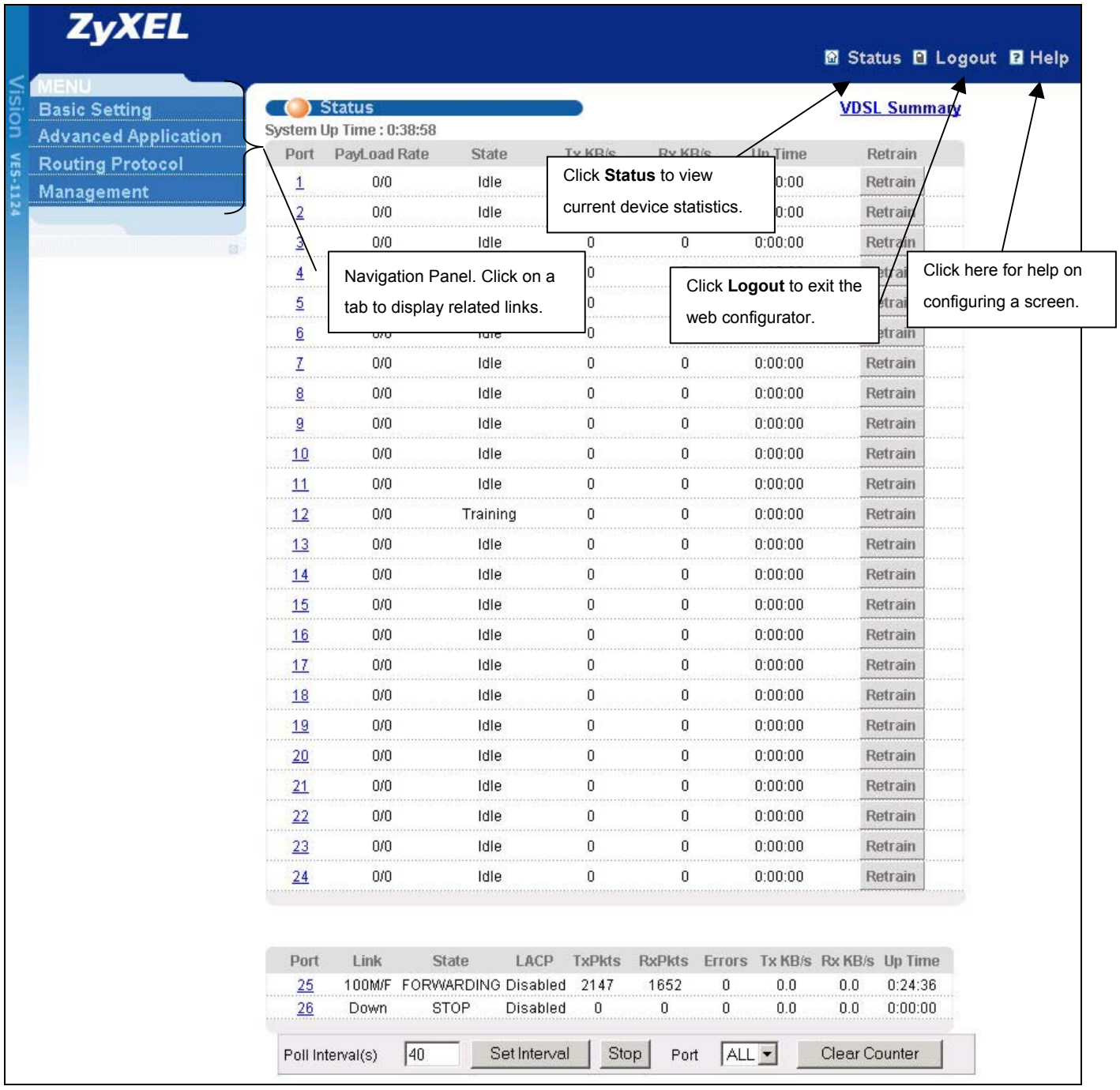
1. Start your Internet Explorer or Netscape Navigator web browser.
2. Type "http://" and the IP address of the switch (for example, the default is 192.168.1.1) in the Location or Address field. Press **Enter**.
3. The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 3-1 Web Configurator: login

4. Click **OK** to view the first web configurator screen.

3.3 Status Screen

The **Status** screen is the first web configurator screen you see after you log in. The following figure shows the navigating components of a web configurator screen.



Port	PayLoad Rate	State	Tx KB/s	Rx KB/s	Up Time	Retrain
1	0/0	Idle			0:00	Retrain
2	0/0	Idle			0:00	Retrain
3	0/0	Idle	0	0	0:00:00	Retrain
4			0			
5			0			
6			0			
7	0/0	Idle	0	0	0:00:00	Retrain
8	0/0	Idle	0	0	0:00:00	Retrain
9	0/0	Idle	0	0	0:00:00	Retrain
10	0/0	Idle	0	0	0:00:00	Retrain
11	0/0	Idle	0	0	0:00:00	Retrain
12	0/0	Training	0	0	0:00:00	Retrain
13	0/0	Idle	0	0	0:00:00	Retrain
14	0/0	Idle	0	0	0:00:00	Retrain
15	0/0	Idle	0	0	0:00:00	Retrain
16	0/0	Idle	0	0	0:00:00	Retrain
17	0/0	Idle	0	0	0:00:00	Retrain
18	0/0	Idle	0	0	0:00:00	Retrain
19	0/0	Idle	0	0	0:00:00	Retrain
20	0/0	Idle	0	0	0:00:00	Retrain
21	0/0	Idle	0	0	0:00:00	Retrain
22	0/0	Idle	0	0	0:00:00	Retrain
23	0/0	Idle	0	0	0:00:00	Retrain
24	0/0	Idle	0	0	0:00:00	Retrain

Port	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
25	100M/F	FORWARDING	Disabled	2147	1652	0	0.0	0.0	0:24:36
26	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

Figure 3-2 Web Configurator Status Screen

In the navigation panel, click a main link to reveal a list of submenu links.

Table 3-1 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL	MANAGEMENT

The following table lists the various web configurator screens within the sub-links.

Table 3-2 Web Configurator Screens Overview

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL	MANAGEMENT
System Info	VLAN	Static Routing	Maintenance
General Setup	VLAN Port Setting		Firmware Upgrade
Switch Setup	Static VLAN		Restore Configuration
IP Setup	Static MAC Forwarding		Backup Configuration
Port Setup	Spanning Tree Protocol		Load Factory Default
VDSL Common Setup	Status		Reboot System
VDSL Profile Setup	Configuration		Diagnostic
	Bandwidth Control		Cluster Management
	Broadcast Storm Control		Status
	Mirroring		Cluster Management Configuration
	Link Aggregation		MAC Table
	Status		ARP Table
	Configuration		
	Port Authentication		
	RADIUS		
	802.1x		
	Port Security		
	Access Control		

Table 3-2 Web Configurator Screens Overview

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL	MANAGEMENT
	SNMP		
	Logins		
	Service Access Control		
	Remote Management		
	Queuing Method		

The following table summarizes the sub-links in the navigation panel.

Table 3-3 Navigation Panel Sub-link Descriptions

LABEL	DESCRIPTION
Basic Setting Screens	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the switch.
Switch Setup	This link takes you to a screen where you can set up global switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for switch management) and DNS (domain name server).
Port Setup	This link takes you to screens where you can configure settings for individual switch ports.
VDSL Common Setup	This link takes you to a screen where you can configure system-wide VDSL settings.
VDSL Profile Setup	This link takes you to a screen where you can configure VDSL profiles.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the **Switch Setup** menu).
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Spanning Tree Protocol	This link takes you to screens where you can configure the STP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed for individual ports.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Link Aggregation	This link takes you to a screen where you can logically trunk physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure RADIUS (Remote Authentication Dial-In User Service), a protocol for user authentication that allows you to use an external server to validate an unlimited number of users.
Port Security	This link takes you to a screen where you can activate MAC address learning.

Table 3-3 Navigation Panel Sub-link Descriptions

LABEL	DESCRIPTION
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Queuing Method	This link takes you to a screen where you can configure first come first serve, strictly priority queuing or weighted round robin scheduling and associated queue weights.
Routing Protocol	
Static Routing	This link takes you to screens where you can configure static routes. A static route defines how the SWITCH should forward traffic by configuring the TCP/IP parameters manually.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Diagnostic	This link takes you to screens where you can view system logs and test port(s).
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.

3.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default Administrator password in the **Logins** screen. Click **Advanced Application**, **Access Control** and then **Logins** to display the next screen.

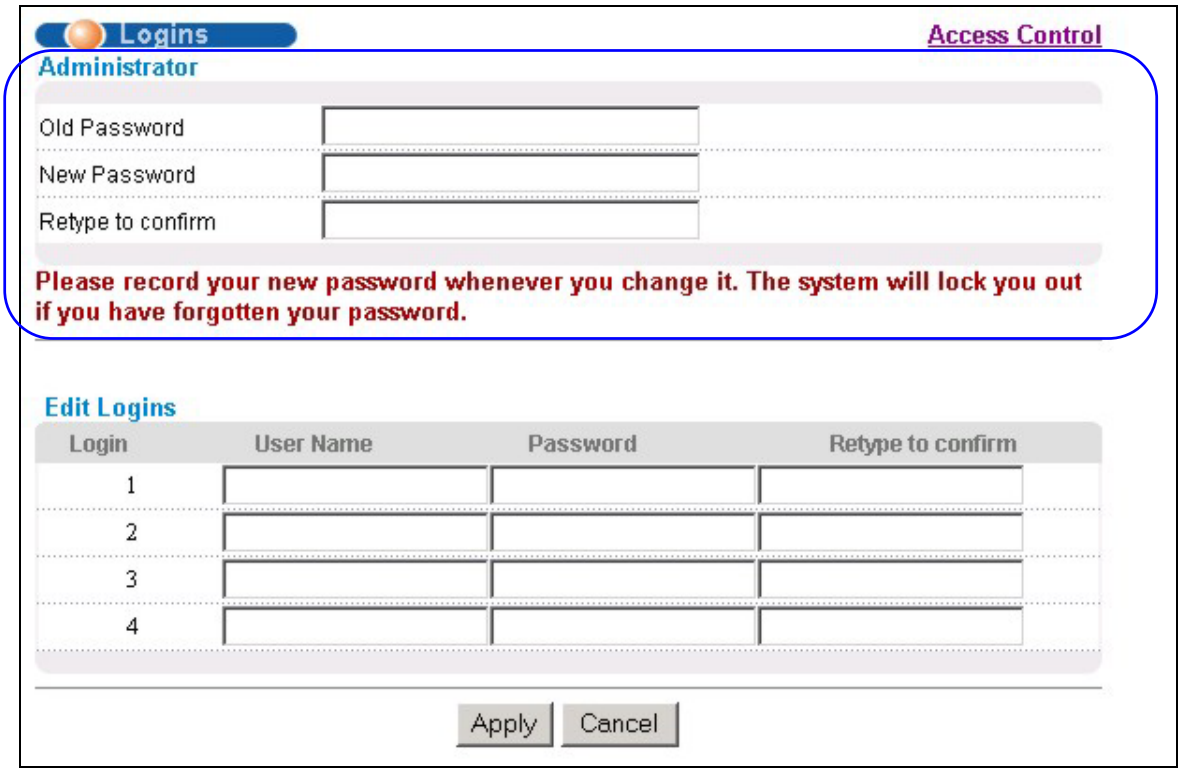


Figure 3-3 Web Configurator: Change Password at Login

3.4 Switch Lockout

You are locked out from managing the switch if another administrator is currently logged in. You must wait until he/she has logged out before you can log in.

Moreover, you could lock yourself (and all others) out from the device by:

1. Deleting the management VLAN (default is VLAN 1).
2. Deleting all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the device.
3. Filtering all traffic to the CPU port.
4. Disabling all ports.
5. Assigning minimum bandwidth to the CPU port. If you limit bandwidth to the CPU port, you may find that the device performs sluggishly or not at all.

Be careful not to lock yourself and others out of the switch.

3.5 Resetting the Switch

If you lock yourself (and others) from the VES, you will need to reload the factory-default configuration file. Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will

be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to "1234" and the IP address to 192.168.1.1.

3.5.1 Resetting the VES Via Command

If you know the VES's password, you can reload the factory-default configuration file via Command Line Interface (CLI) command. Use the following procedure.

1. Connect to the console port using a computer with terminal emulation software. See the chapter on hardware connections for details.
2. Enter your password.
3. Type `sys romreset`.
4. Type `y` at the question "`Do you want to restore default ROM file(y/n)?`"
5. The device restarts.

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
VES-1124> sys romreset
Do you want to restore default ROM file(y/n)?y
Restore default Romfile.
OK

System Restart! (Console speed will be changed to 9600 bps)
VES-1124>
Bootbase Version: V1.00(VES-1124) | 04/26/2004 17:12:37
RAM: Size = 16384 Kbytes
FLASH: Intel 16M

ZyNOS Version: V3.50(LP.0)b2 | 05/18/2004 14:45:01

Press any key to enter debug mode within 3 seconds.
.....................................................
     (Compressed)
     Version: RAS VES1124, start: 02049030
     Length: 2F24F0, Checksum: 92A1
     Compressed Length: EB713, Checksum: 6ABB
```

Figure 3-4 Resetting the VES Via Command

The switch is now reinitialized with a default configuration file including the default password of "1234".

3.5.2 Uploading the Default Configuration File Via Console Port

If you forget the VES's password, you will need to reload the factory-default configuration file via console port. Use the following procedure.

1. Connect to the console port using a computer with terminal emulation software. See the chapter on hardware connections for details.
2. Disconnect and reconnect the VES's power to begin a session. When you reconnect the switch's power, you will see the initial screen.
3. When you see the message "`Press any key to enter Debug Mode within 3 seconds`" press any key to enter debug mode.

4. Type `atlc` after the "`Enter Debug Mode`" message.
5. Wait for the "`Starting XMODEM upload`" message before activating XMODEM upload on your terminal.
6. After a successful configuration file upload, type `atgo` to restart the VES.

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
VES-1124>
Bootbase Version: V1.00(VES-1124) | 04/26/2004 17:12:37
RAM: Size = 16384 Kbytes
DRAM POST: Testing: 16384K OK
FLASH: Intel 16M

ZyNOS Version: V3.50(LP.0)b2 | 05/18/2004 14:45:01

Press any key to enter debug mode within 3 seconds.
.................
Enter Debug Mode
ZyDbg>atlc

Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCC
Total  262144 bytes received.

Erasing..
.............................................................
OK
```

Figure 3-5 Uploading the Default Configuration File Via Console Port

The VES is now reinitialized with a default configuration file including the default password of "1234".

3.5.3 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so as you don't lock out other VES administrators.

Figure 3-6 Web Configurator: Logout Screen

3.5.4 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from the home screen to view the online help's home screen summary menu.

Click the **Help** link from a web configurator screen other than the home screen to view an online help description of that screen.

Chapter 4
Status, Port Details and VDSL Summary

This chapter describes the system status (web configurator home page) and port details screens.

4.1 Overview

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details. You can also access the summary screen for the VDSL status.

4.2 Port Status

To view the port statistics, click **Status** in any web configurator screen to display the **Status** screen as shown next.

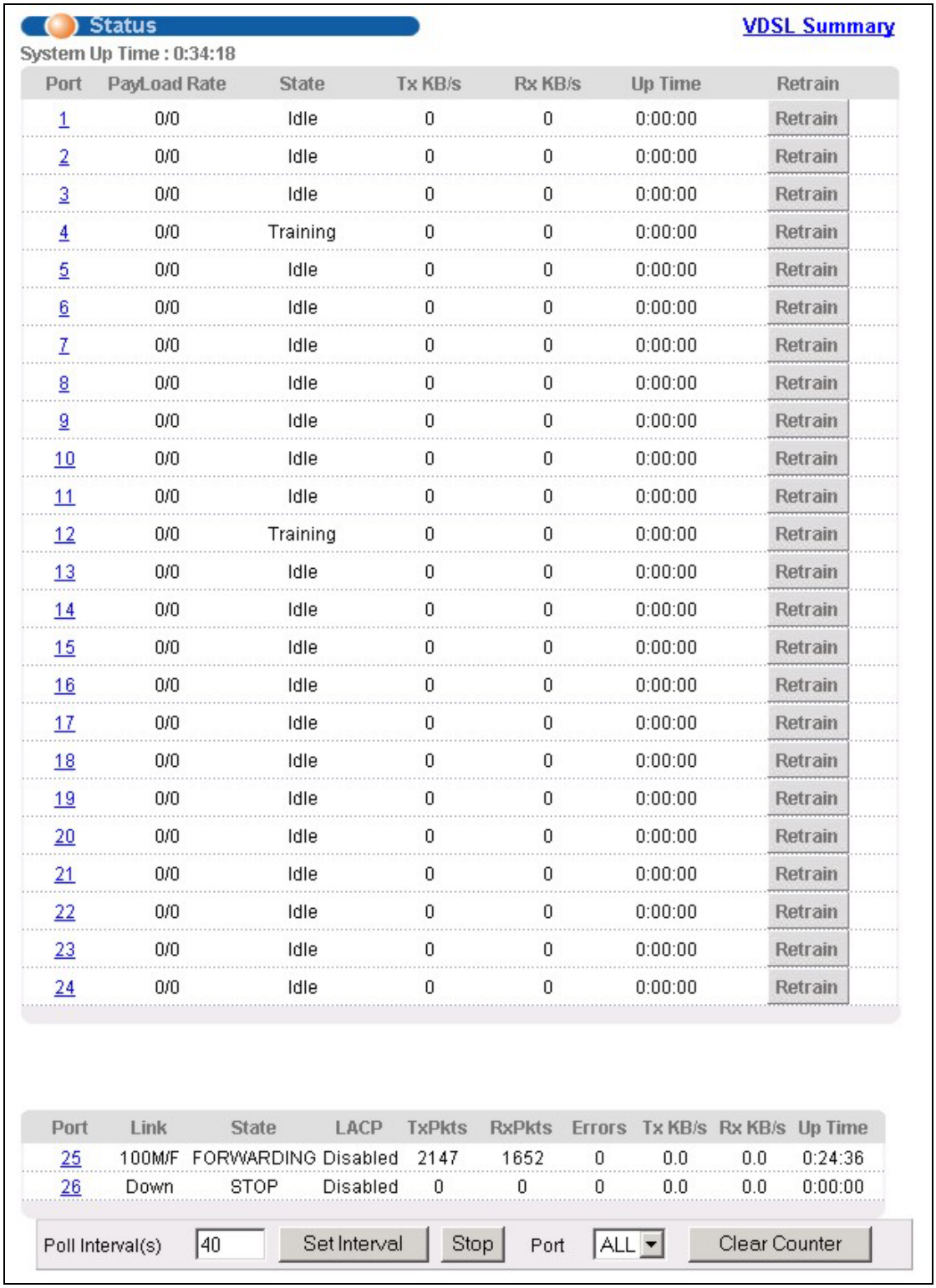

Status
VDSL Summary
System Up Time : 0:34:18
Port PayLoad Rate State Tx KB/s Rx KB/s Up Time Retrain
1 0/0 Idle 0 0 0:00:00 Retrain
2 0/0 Idle 0 0 0:00:00 Retrain
3 0/0 Idle 0 0 0:00:00 Retrain
4 0/0 Training 0 0 0:00:00 Retrain
5 0/0 Idle 0 0 0:00:00 Retrain
6 0/0 Idle 0 0 0:00:00 Retrain
7 0/0 Idle 0 0 0:00:00 Retrain
8 0/0 Idle 0 0 0:00:00 Retrain
9 0/0 Idle 0 0 0:00:00 Retrain
10 0/0 Idle 0 0 0:00:00 Retrain
11 0/0 Idle 0 0 0:00:00 Retrain
12 0/0 Training 0 0 0:00:00 Retrain
13 0/0 Idle 0 0 0:00:00 Retrain
14 0/0 Idle 0 0 0:00:00 Retrain
15 0/0 Idle 0 0 0:00:00 Retrain
16 0/0 Idle 0 0 0:00:00 Retrain
17 0/0 Idle 0 0 0:00:00 Retrain
18 0/0 Idle 0 0 0:00:00 Retrain
19 0/0 Idle 0 0 0:00:00 Retrain
20 0/0 Idle 0 0 0:00:00 Retrain
21 0/0 Idle 0 0 0:00:00 Retrain
22 0/0 Idle 0 0 0:00:00 Retrain
23 0/0 Idle 0 0 0:00:00 Retrain
24 0/0 Idle 0 0 0:00:00 Retrain
Port Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Time
25 100M/F FORWARDING Disabled 2147 1652 0 0.0 0.0 0:24:36
26 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
Poll Interval(s) 40 Set Interval Stop Port ALL Clear Counter

Figure 4-1 Status

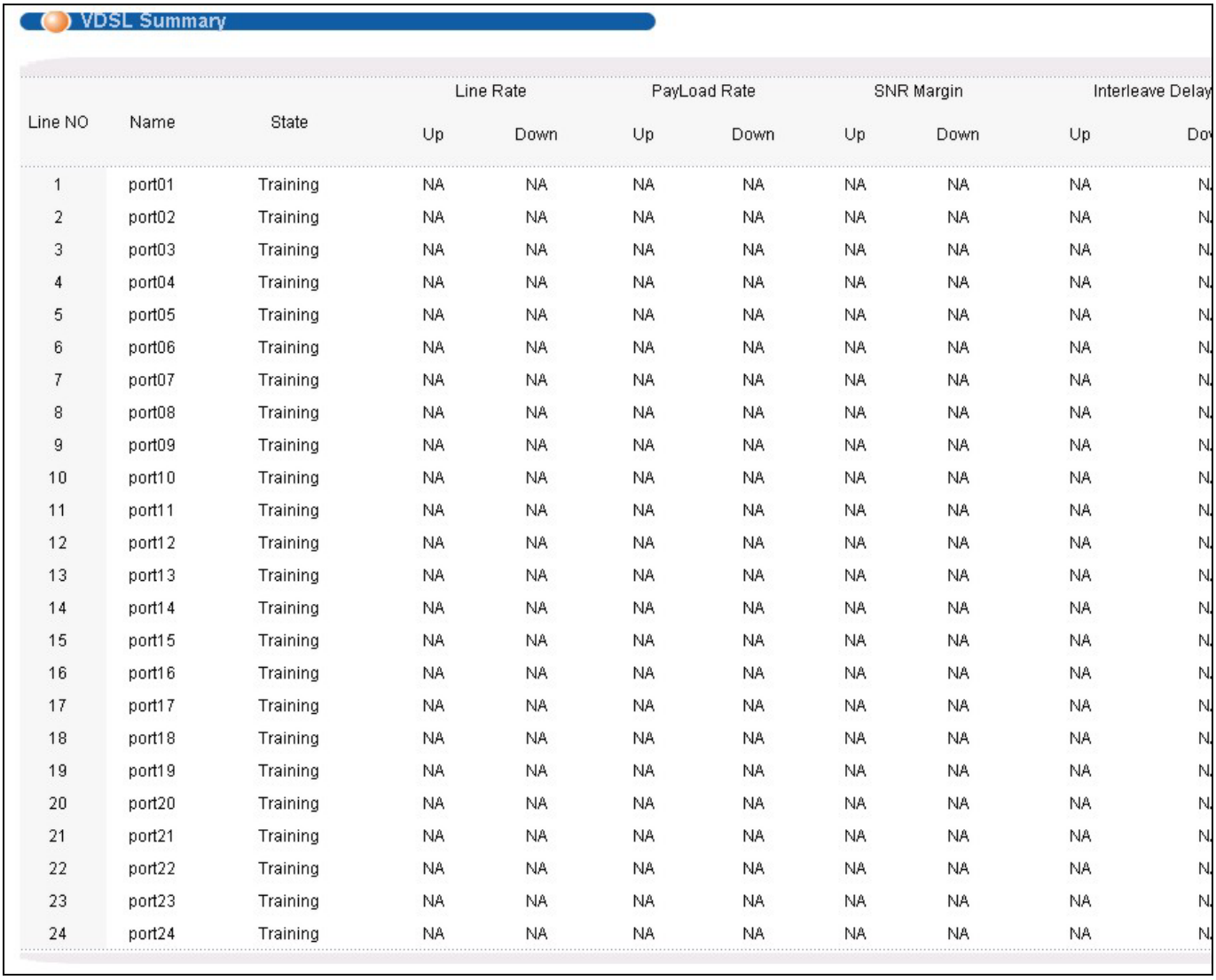
The following table describes the labels in this screen.

Table 4-1 Status

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
The following fields are related to the VDSL ports.	
Port	This identifies the VDSL port. Click a port number to display the **VDSL Port Details** screen (refer to *Figure 4-3*).
PayLoad Rate	This field displays the upstream and downstream payload rates.
State	This field shows whether the port is connected (**Showtime**), not connected (**Idle**) or is negotiating a connection (**Training**).
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Retrain	Click **Retrain** to re-establish line connection.
The following fields are related to the Ethernet port.	
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to *Section 4.2.1*).
Link	This field displays the speed (either **10M** for 10Mbps or **100M** for 100Mbps) and the duplex (**F** for full duplex or **H** for half) and displays **Down** when the line is down or not connected.
State	This field displays the STP (Spanning Tree Protocol) state (disabled, listening, blocking, learning or forwarding) of the port.
LACP	This fields displays whether the Link Aggregation Control Protocol (LACP) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.

4.2.1 VDSL Summary

To view VDSL statistics, click **VDSL Summary** in the **Status** screen.



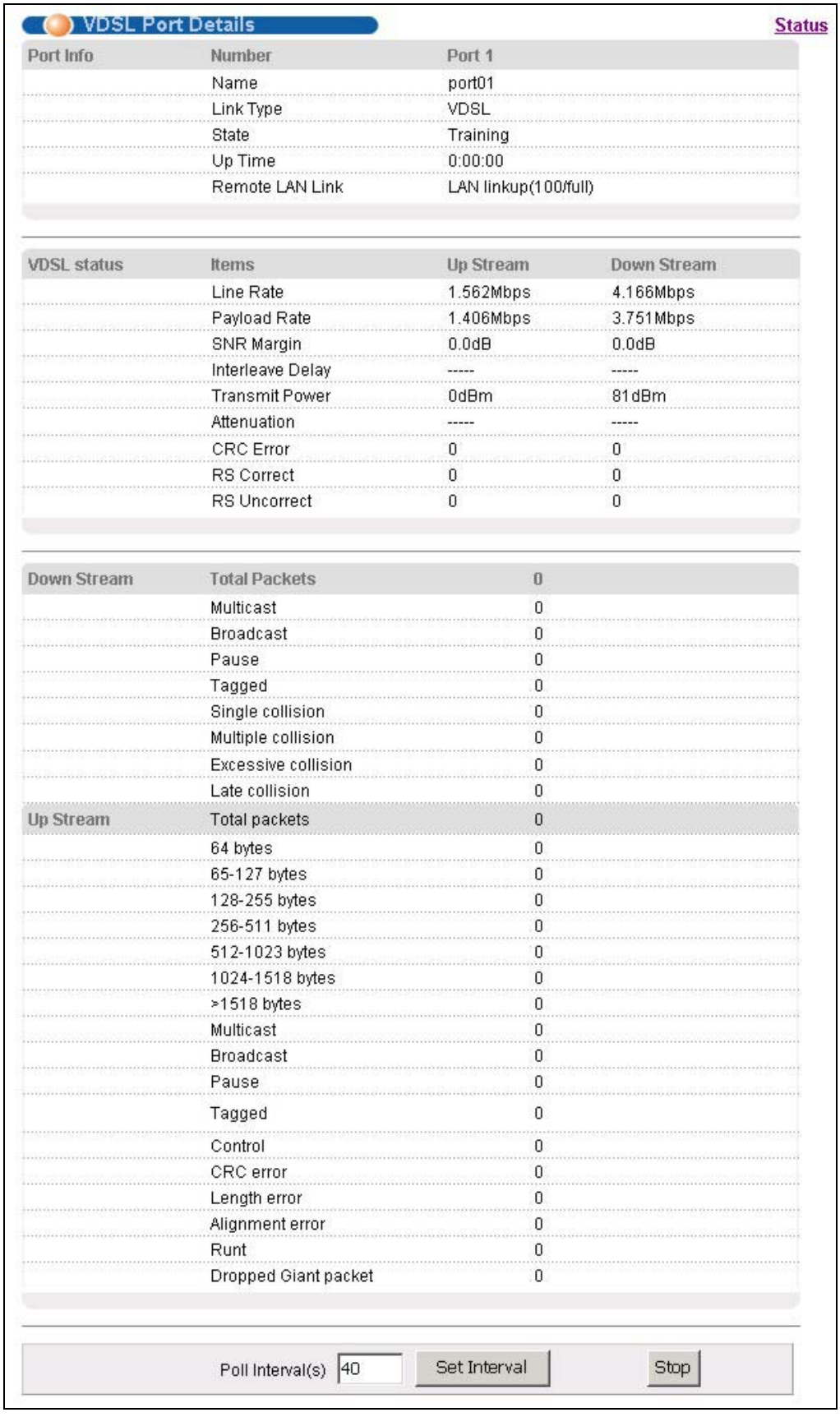
VDSL Summary

Line NO	Name	State	Line Rate		PayLoad Rate		SNR Margin		Interleave Delay	
			Up	Down	Up	Down	Up	Down	Up	Do
1	port01	Training	NA	NA	NA	NA	NA	NA	NA	N
2	port02	Training	NA	NA	NA	NA	NA	NA	NA	N
3	port03	Training	NA	NA	NA	NA	NA	NA	NA	N
4	port04	Training	NA	NA	NA	NA	NA	NA	NA	N
5	port05	Training	NA	NA	NA	NA	NA	NA	NA	N
6	port06	Training	NA	NA	NA	NA	NA	NA	NA	N
7	port07	Training	NA	NA	NA	NA	NA	NA	NA	N
8	port08	Training	NA	NA	NA	NA	NA	NA	NA	N
9	port09	Training	NA	NA	NA	NA	NA	NA	NA	N
10	port10	Training	NA	NA	NA	NA	NA	NA	NA	N
11	port11	Training	NA	NA	NA	NA	NA	NA	NA	N
12	port12	Training	NA	NA	NA	NA	NA	NA	NA	N
13	port13	Training	NA	NA	NA	NA	NA	NA	NA	N
14	port14	Training	NA	NA	NA	NA	NA	NA	NA	N
15	port15	Training	NA	NA	NA	NA	NA	NA	NA	N
16	port16	Training	NA	NA	NA	NA	NA	NA	NA	N
17	port17	Training	NA	NA	NA	NA	NA	NA	NA	N
18	port18	Training	NA	NA	NA	NA	NA	NA	NA	N
19	port19	Training	NA	NA	NA	NA	NA	NA	NA	N
20	port20	Training	NA	NA	NA	NA	NA	NA	NA	N
21	port21	Training	NA	NA	NA	NA	NA	NA	NA	N
22	port22	Training	NA	NA	NA	NA	NA	NA	NA	N
23	port23	Training	NA	NA	NA	NA	NA	NA	NA	N
24	port24	Training	NA	NA	NA	NA	NA	NA	NA	N

Figure 4-2 Status: VDSL Summary

4.2.2 The Port Details Screens

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the switch.



VDSL Port Details

Status

Port Info	Number	Port 1
	Name	port01
	Link Type	VDSL
	State	Training
	Up Time	0:00:00
	Remote LAN Link	LAN linkup(100/full)

VDSL status	Items	Up Stream	Down Stream
	Line Rate	1.562Mbps	4.166Mbps
	Payload Rate	1.406Mbps	3.751Mbps
	SNR Margin	0.0dB	0.0dB
	Interleave Delay	-----	-----
	Transmit Power	0dBm	81dBm
	Attenuation	-----	-----
	CRC Error	0	0
	RS Correct	0	0
	RS Uncorrect	0	0

Down Stream	Total Packets	0
	Multicast	0
	Broadcast	0
	Pause	0
	Tagged	0
	Single collision	0
	Multiple collision	0
	Excessive collision	0
	Late collision	0
Up Stream	Total packets	0
	64 bytes	0
	65-127 bytes	0
	128-255 bytes	0
	256-511 bytes	0
	512-1023 bytes	0
	1024-1518 bytes	0
	>1518 bytes	0
	Multicast	0
	Broadcast	0
	Pause	0
	Tagged	0
	Control	0
	CRC error	0
	Length error	0
	Alignment error	0
	Runt	0
	Dropped Giant packet	0

Poll Interval(s) 40 Set Interval Stop

Figure 4-3 Status: VDSL Port Details

The following table describes the labels in this screen.

Table 4-2 Status: VDSL Port Details

LABEL	DESCRIPTION
Port Info	
Number	This field displays the port number.
Name	This field displays the descriptive name of a port.
Link Type	This field displays the type of the port.
State	This field displays whether the port is connected (**Showtime**), not connected (**Idle**) or is negotiating a connection (**Training**).
Up Time	This field shows the total amount of time the line has been up.
Remote LAN Link	This field displays the status of the link to the remote CPE device.
VDSL Status	
Line Rate	This field displays the upstream/downstream transmission rate.
Payload Rate	This field displays the upstream/downstream payload rate.
SNR Margin	This field displays the upstream/downstream SNR margin.
Interleave Delay	This field displays the upstream/downstream interleave delay.
Transmit Power	This field displays the upstream/downstream transmission power of the line.
Attenuation	This field displays the upstream/downstream attenuation.
CRC Error	This field displays the number of CRC (Cyclical Redundancy Check) error packet.
RS Correct	This field displays the number of Reed-Solomon (RS) correct packets.
RS Uncorrect	This field displays the number of Reed-Solomon (RS) uncorrect packets.
Down Stream The following fields display detailed information about packets received.	
Total Packets	This field shows the total number of frames (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause frames received.
Tagged	This field shows the number of frames with VLAN tags transmitted.
Single Collision	This field shows the number of packets with 1 collision detected.
Multiple Collision	This field shows the number of packets with 2 to 15 collisions detected.

Table 4-2 Status: VDSL Port Details

LABEL	DESCRIPTION
Excessive Collision	This field shows the number of packets with in excess of 15 collisions detected.
Late Collision	A late collision is counted when a device detects a collision after it has sent the 512th bit of its frame. This field shows the number of times such a collision is detected.
Up Stream The following fields display detailed information about packets transmitted.	
Total Packets	This field shows the total number of frames (unicast, multicast and broadcast) transmitted.
64 bytes	This field shows the number of packets (including bad packets) transmitted that were 64 octets in length.
65-127 bytes	This field shows the number of packets (including bad packets) transmitted that were between 65 and 127 octets in length.
128-255 bytes	This field shows the number of packets (including bad packets) transmitted that were between 128 and 255 octets in length.
256-511 bytes	This field shows the number of packets (including bad packets) transmitted that were between 256 and 511 octets in length.
512-1023 bytes	This field shows the number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length.
1024-1518 bytes	This field shows the number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length.
>1518 bytes	This field shows the number of packets (including bad packets) transmitted that were longer than 1518 octets in length.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause frames transmitted.
Tagged	This field shows the number of frames with VLAN tags transmitted.
Control	This field shows the number of control sent (including those with CRC error) but it does not include the 802.3x Pause frames.
CRC Error	This field shows the number of frames with CRC (Cyclic Redundant Check) error(s).
Length Error	This field shows the number of frames with a length that was out of range.
Alignment	This field shows the number of packets received of proper size but with CRC error(s) and a non-integral number of octets.
Runt	This field shows the number of frames received that were too short (shorter than 64 octets), including the ones with CRC errors.

Table 4-2 Status: VDSL Port Details

LABEL	DESCRIPTION
Dropped giant packet	This field shows the number of frames dropped because they were bigger than the maximum frame size.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to stop port statistic polling.

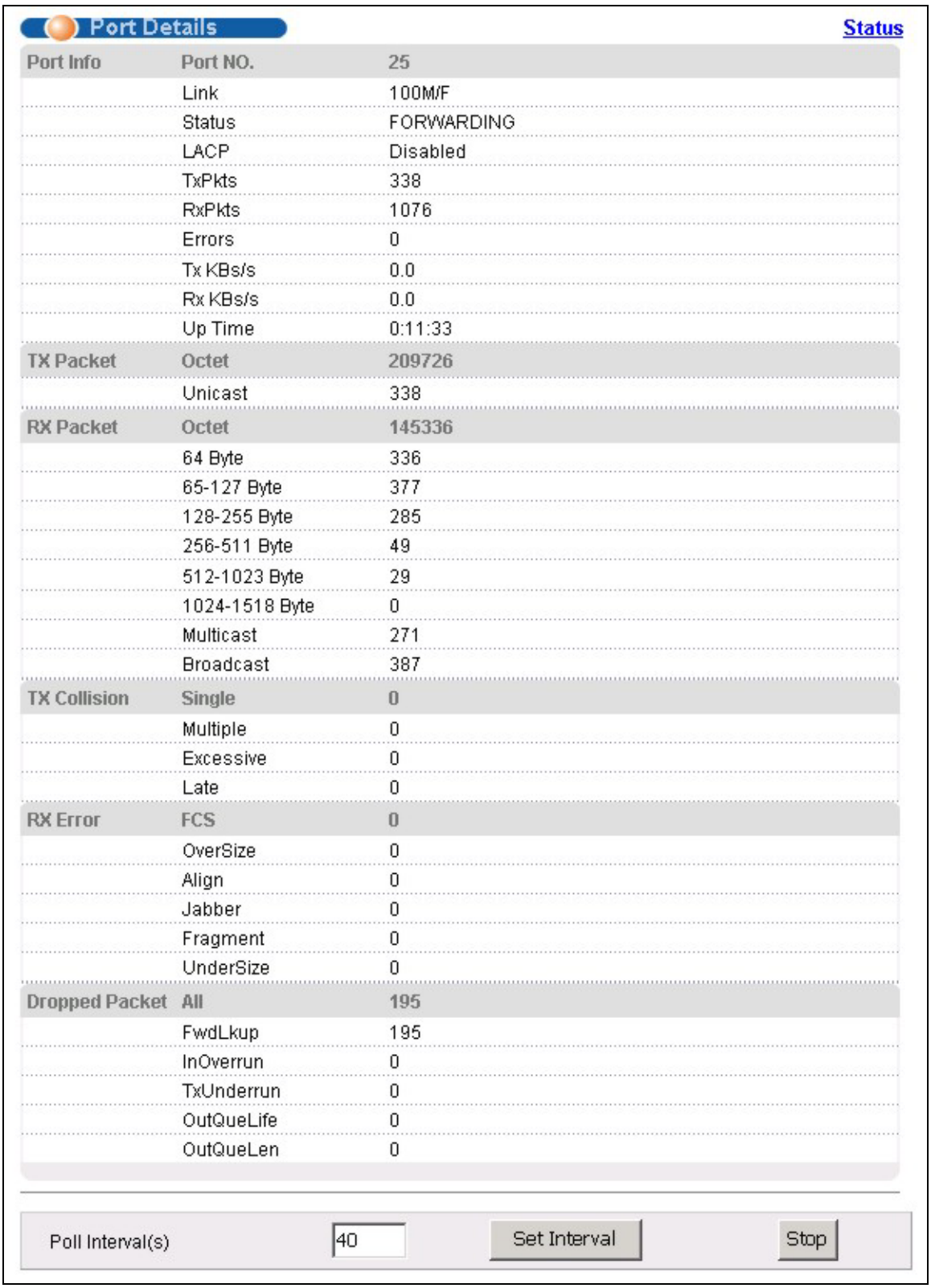


Figure 4-4 Status: Port Details (Ethernet)

The following table describes the labels in this screen.

Table 4-3 Status: Port Details (Ethernet)

LABEL	DESCRIPTION
Port Info	
Port NO.	This field identifies the Ethernet port described in this screen.
Link	This field shows whether the Ethernet connection is down, and the speed/duplex mode.
Status	This field shows the training state of the ports. The states are **FORWARDING** (forwarding), which means the link is functioning normally or **STOP** (the port is stopped to break a loop or duplicate path).
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KBs/s	This field shows the number kilobytes per second transmitted on this port.
Rx KBs/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about frames transmitted.	
Octet	This field shows the number of octets transmitted.
Unicast	This field shows the number of good unicast packets received.
Rx Packet The following fields display detailed information about frames received.	
Octet	This field shows the number of octets received.
64 Byte	This field shows the number of frames (including bad frames) received that were 64 octets in length.
65-127 Byte	This field shows the number of frames (including bad frames) received that were between 65 and 127 octets in length.
128-255 Byte	This field shows the number of frames (including bad frames) received that were between 128 and 255 octets in length.
256-511 Byte	This field shows the number of frames (including bad frames) received that were between 256 and 511 octets in length.
512-1023 Byte	This field shows the number of frames (including bad frames) received that were between 512 and 1023 octets in length.
1024-1518 Byte	This field shows the number of frames (including bad frames) received that were between 1024 and 1518 octets in length.

Table 4-3 Status: Port Details (Ethernet)

LABEL	DESCRIPTION
Multicast	This field shows the number of good multicast frames received.
Broadcast	This field shows the number of good broadcast frames received.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frame have already been transmitted.
RX Error The following fields display detailed information about frames received with error.	
FCS	This field shows the number of frames received of the proper size but with CRC error(s) and a non-integral number of octets.
OverSize	This field shows the number of packets received that were bigger than the maximum frame size.
Align	This field shows the number of frames received of proper size but with CRC error(s) and a non-integral number of octets.
Jabber	This field shows the number of frames received that were greater than the maximum octets (specified for the system by the configuration software) long and with either CRC or alignment error(s).
Fragment	This field shows the number of packets received that were less than 64 octets long, and with either CRC (Cyclic Redundant Check) or alignment error(s).
UnderSize	This field shows the number of frames received that were less than 64 octets long and without CRC error(s) or alignment error(s).
Dropped Packet The following fields display detailed information about frames that were dropped.	
All	This field shows the total number of frames that were dropped.
FwdLkup	This field shows the number of unicast packets that were dropped after the forwarding table lookup.
InOverrun	This field shows the number of the incoming packets that were dropped because of an input FIFO overrun.

Table 4-3 Status: Port Details (Ethernet)

LABEL	DESCRIPTION
TxUnderrun	This field shows the number of outgoing packets that were dropped because of output buffer underrun.
OutQueLife	This field shows the number of packets that were dropped because the queue time was longer than the lifetime setting.
OutQueLen	This field shows the number of packets in the SWITCH's output queue, waiting for transmission.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to stop port statistic polling.

Chapter 5 Basic Setting

*This chapter describes how to configure the **System Info**, **General Setup**, **Switch Setup**, **IP Setup**, **Port Setup**, **VDSL Common Setup** and **VDSL Profile Setup** screens.*

5.1 Introducing The Basic Setting Screens

The **System Info** screen displays general switch information (such as firmware version number) and hardware polling information (such as temperature). The **General Setup** screen allows you to configure general switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure a switch IP address, subnet mask and DNS (domain name server) for management purposes. Use the **VDSL Common Setup** and **VDSL Profile Setup** screen to configure VDSL settings and profiles.

5.2 System Information

In the navigation panel, click **Basic Setting** and then **System Info** to display the screen as shown. You can check the firmware version number and monitor the switch fan status in this screen.

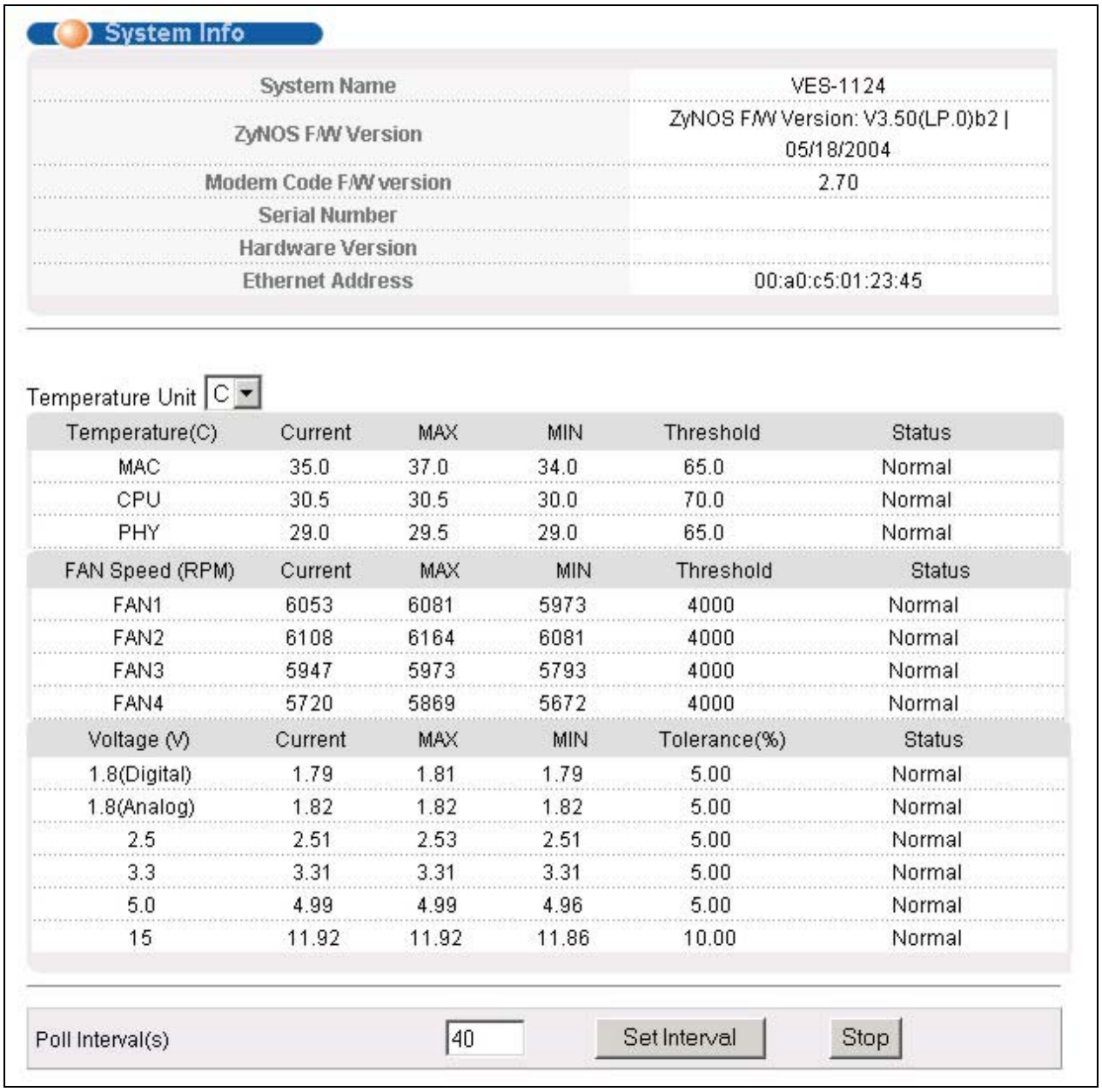

System Info
System Name
VES-1124
ZyNOS F/W Version
ZyNOS F/W Version: V3.50(LP.0)b2 | 05/18/2004
Modem Code F/W version
2.70
Serial Number
Hardware Version
Ethernet Address
00:a0:c5:01:23:45
Temperature Unit C
Temperature(C) Current MAX MIN Threshold Status
MAC 35.0 37.0 34.0 65.0 Normal
CPU 30.5 30.5 30.0 70.0 Normal
PHY 29.0 29.5 29.0 65.0 Normal
FAN Speed (RPM) Current MAX MIN Threshold Status
FAN1 6053 6081 5973 4000 Normal
FAN2 6108 6164 6081 4000 Normal
FAN3 5947 5973 5793 4000 Normal
FAN4 5720 5869 5672 4000 Normal
Voltage (V) Current MAX MIN Tolerance(%) Status
1.8(Digital) 1.79 1.81 1.79 5.00 Normal
1.8(Analog) 1.82 1.82 1.82 5.00 Normal
2.5 2.51 2.53 2.51 5.00 Normal
3.3 3.31 3.31 3.31 5.00 Normal
5.0 4.99 4.99 4.96 5.00 Normal
15 11.92 11.92 11.86 10.00 Normal
Poll Interval(s)
40
Set Interval
Stop

Figure 5-1 System Info

The following table describes the labels in this screen.

Table 5-1 System Info

LABEL	DESCRIPTION
System Name	This field displays the switch 's model name.
ZyNOS F/W Version	This field displays the version number of the switch's current firmware including the date created.
Modem Code F/W Version	This field displays the version number of the switch 's current modem code version.

Table 5-1 System Info

LABEL	DESCRIPTION
Serial Number	This field displays the serial number of your switch.
Hardware Version	This field displays the hardware version number of your switch.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.
Temperature Unit	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**MAC**, **CPU** and **PHY** refer to the location of the temperature sensors on the switch printed circuit board.
Current	This field displays the current temperature measured at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM). "<41" is displayed for speeds equal to 0 RPM if the fan is removed or cannot work.
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the threshold. **Error** indicates that this fan is functioning below the threshold.
Voltage (V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Tolerance (%)	This field displays the voltage tolerance.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.

Table 5-1 System Info

LABEL	DESCRIPTION
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Set Interval	You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

5.3 General Setup

Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown.

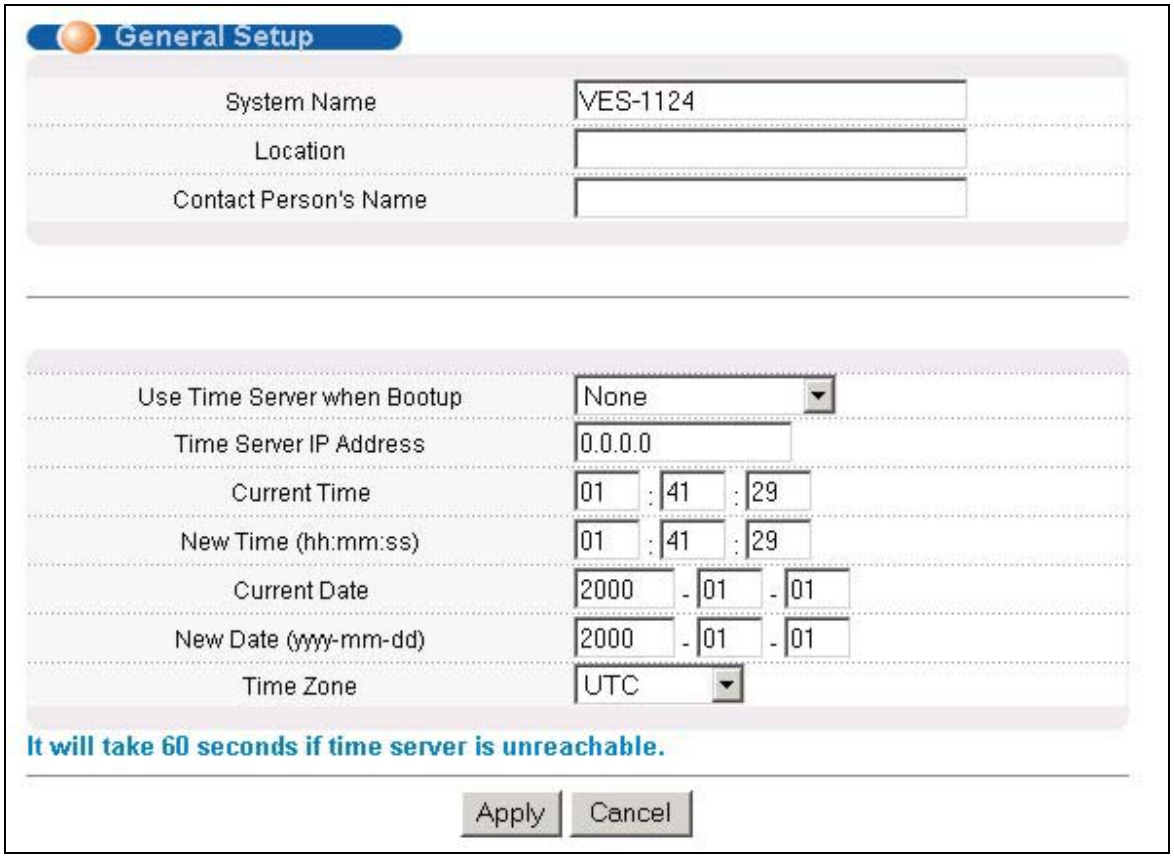


Figure 5-2 General Setup

The following table describes the labels in this screen.

Table 5-2 General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 32 printable characters; spaces are not allowed.

Table 5-2 General Setup

LABEL	DESCRIPTION
Location	Enter the geographic location (up to 30 characters) of your switch.
Contact Person's Name	Enter the name (up to 30 characters) of the person in charge of this switch.
Use Time Server When Bootup	Enter the time service protocol that a timeserver sends when you turn on the switch. Not all timeservers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 2000-1-1 0:0.
Time Server IP Address	Enter the IP address (or URL if you configure a domain name server in the IP Setup screen) of your timeserver. The SWITCH searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring the screen again.

5.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that VLAN is unidirectional; it only governs outgoing traffic.

See the *VLAN* chapter for information on port-based and 802.1Q tagged VLANs.

5.5 IGMP Snooping

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to *RFC 1112* and *RFC 2236* for information on IGMP versions 1 and 2 respectively.

A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, group multicast traffic is only forwarded to ports that are members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your VES.

5.6 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLANs.

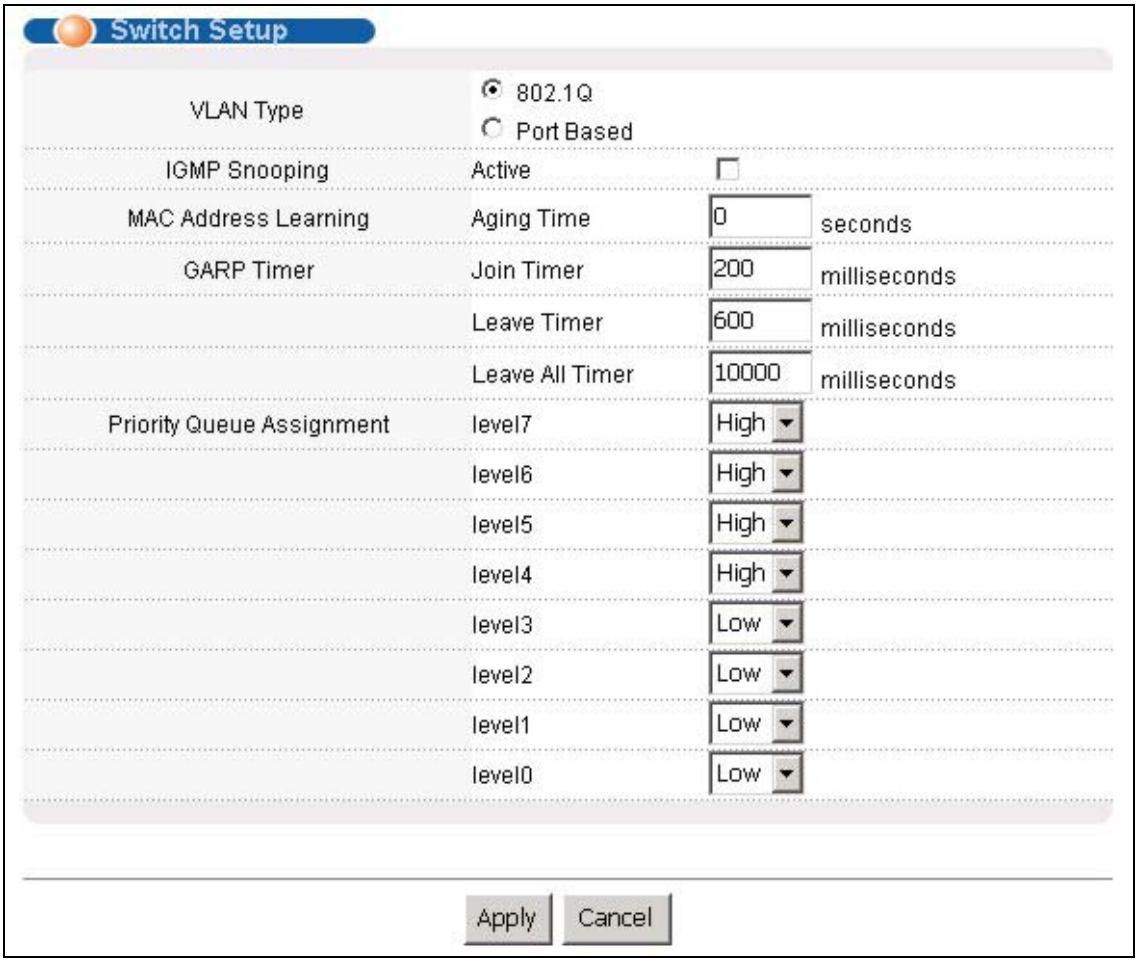


Figure 5-3 Switch Setup

The following table describes the labels in this screen.

Table 5-3 Switch Setup

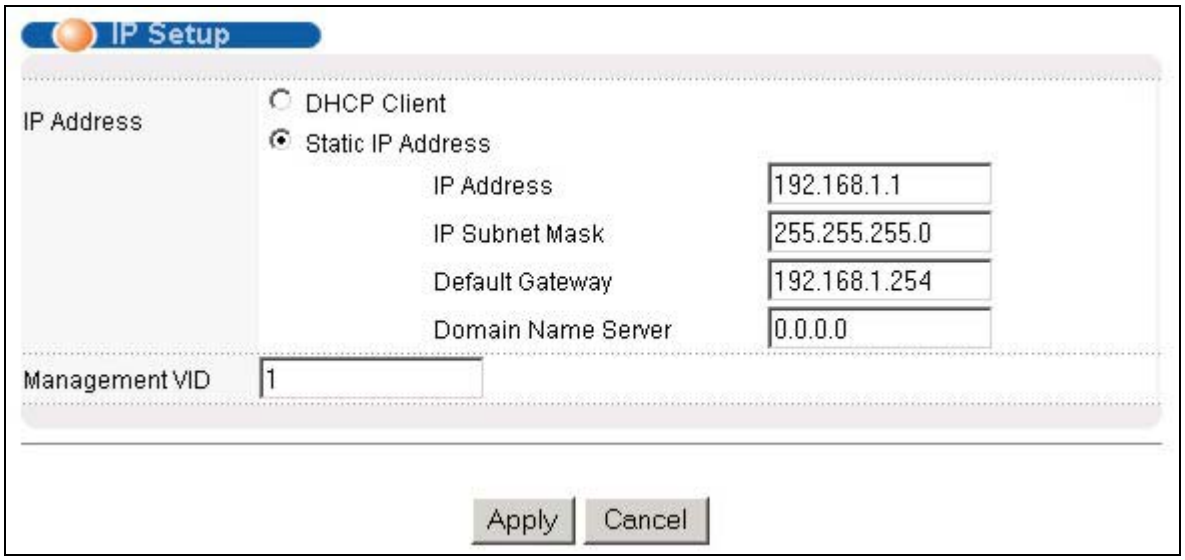
LABEL	DESCRIPTION
VLAN Type	Choose **802.1Q** or **Port Based** from the drop-down list box. The **VLAN Setup** screen changes depending on whether you choose **802.1Q VLAN Type** or **Port Based VLAN Type** in this screen. See *Section 5.4* and the *VLAN* chapter for more information on VLANs.
IGMP Snooping	Select **Active** to enable IGMP snooping have group multicast traffic only forwarded to ports that are members of the VLAN, significantly reducing multicast traffic passing through your SWITCH. See *Section 5.5* for more information on IGMP snooping.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 765 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).

Table 5-3 Switch Setup

LABEL	DESCRIPTION
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Timer sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 1000 milliseconds.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. The switch has two physical queues that you can map to the eight priority levels. On the switch, traffic assigned to the high priority queue gets through faster while traffic in the low priority queue is dropped if the network is congested. See also **Queuing Method** and **802.1p Priority** in **Port Setup** for related information.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for "spare bandwidth".
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.7 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains.



To set the default gateway device and the domain name server on the switch, click **IP Setup** in the navigation panel and set the related fields. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

The following table describes the labels in this screen.

Table 5-4 IP Setup

LABEL	DESCRIPTION
DHCP Client	Select this option if you have a DHCP server that can assign the switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.

Table 5-4 IP Setup

LABEL	DESCRIPTION
Management VID	Enter the VLAN identification number associated with the switch IP address. Management VLAN ID is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the switch, make sure the port that you are connected to is a member of Management VLAN.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring the fields again.

5.8 Port Setup

Click **Basic Setting** and then **Port Setup** in the navigation panel to enter the port configuration screen. You may configure any of the VDSL ports including the Ethernet port.

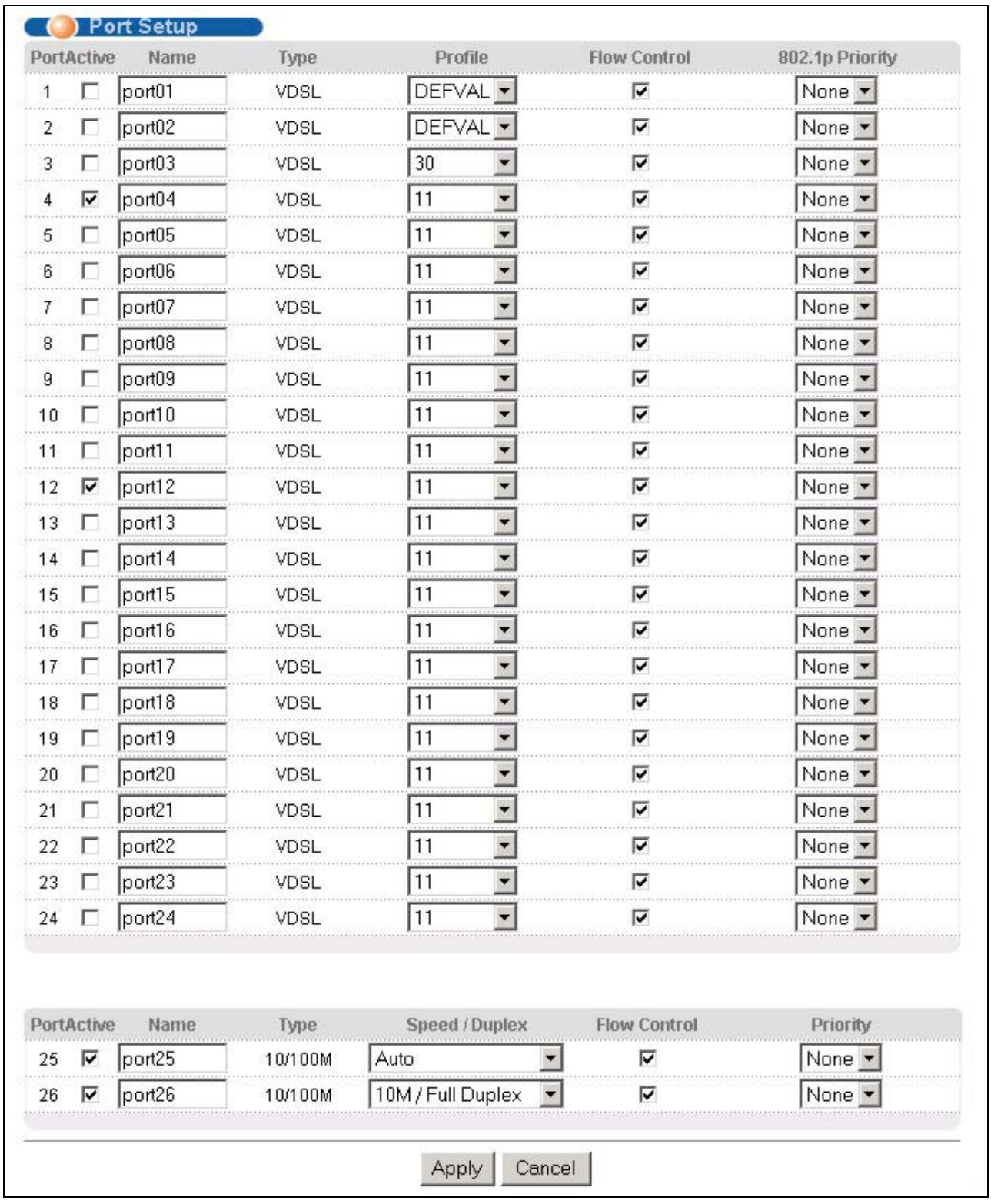

Port Setup
Port Active Name Type Profile Flow Control 802.1p Priority
1 port01 VDSL DEFVAL None
2 port02 VDSL DEFVAL None
3 port03 VDSL 30 None
4 port04 VDSL 11 None
5 port05 VDSL 11 None
6 port06 VDSL 11 None
7 port07 VDSL 11 None
8 port08 VDSL 11 None
9 port09 VDSL 11 None
10 port10 VDSL 11 None
11 port11 VDSL 11 None
12 port12 VDSL 11 None
13 port13 VDSL 11 None
14 port14 VDSL 11 None
15 port15 VDSL 11 None
16 port16 VDSL 11 None
17 port17 VDSL 11 None
18 port18 VDSL 11 None
19 port19 VDSL 11 None
20 port20 VDSL 11 None
21 port21 VDSL 11 None
22 port22 VDSL 11 None
23 port23 VDSL 11 None
24 port24 VDSL 11 None
Port Active Name Type Speed / Duplex Flow Control Priority
25 port25 10/100M Auto None
26 port26 10/100M 10M / Full Duplex None
Apply
Cancel

Figure 5-4 Port Setup

The following table describes the labels in this screen.

Table 5-5 Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
Active	Select this check box to enable a port. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port.
Type	This field displays either **VDSL** or **10/100M** for port type.
Profile	This is a pre-configured profile associated with your port. Select a VDSL profile from the drop down-list box. Use the **VDSL Profile Setup** screen to configure a new profile or edit an existing profile. Refer to *Section 5.11* for more information.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex** and **100M/Full Duplex**. Selecting **Auto** (auto-negotiation) makes one Ethernet port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, an Ethernet port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select this option to enable it.
802.1p Priority	Use this field to specify to which queue the switch assigns the (tagged or untagged) packets received on this port. This overrides the switch's device-wide IEEE 802.1p priority level to queue mapping (see **Priority Queue Assignment** in *Table 5-3* for more information. Select **High** to assign the packets to the high priority queue. Select **Low** to assign the packets to the low priority queue. Traffic assigned to the high priority queue gets through faster while traffic in the low priority queue is dropped if the network is congested. See also **Queuing Method** for related information. Select **None** to forward the tagged packets based on the priority level in their tags. By default the switch treats untagged packets as priority level 0.
Apply	Click **Apply** to save your changes back to the switch.

Table 5-5 Port Setup

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.9 VDSL Parameters

The following sections describe the VDSL parameters you configure in the **VDSL Common Setup** and the **VDSL Profile Setup** screens.

5.9.1 Frequency Band Plans

Each VDSL mode operates in a different frequency band allocation, resulting in different upstream and downstream speeds.

- 10BaseS giving upstream rates from 1.56 Mbps to 18.75 Mbps and downstream rates of 4.17 Mbps to 16.67 Mbps.
- ANSI/ETSI Plan 998 Mode giving upstream rates from 1.56 Mbps to 6.25 Mbps and downstream rates of 4.17 Mbps to 16.67 Mbps.
- ETSI Plan 997 Mode giving upstream rates from 1.56 Mbps to 6.25 Mbps and downstream rates of 4.17 Mbps to 12.50Mbps.

Configured Versus Actual Rate

You configure the maximum rate of an individual VDSL port by modifying its profile (see the **VDSL Profile Setup** screen) or assigning the port to a different profile (see the **Port Setup** screen). However, the actual rate varies depending on factor such as transmission range and interference.

5.9.2 PSD and PBO

PSD (Power Spectral Density) defines the distribution of a VDSL line's power in the frequency domain. A PSD mask is a template that specifies the maximum allowable PSD for a line.

In a network with varying telephone wiring lengths, the PSD on each line is different. This causes crosstalk between the lines. Enable PBO (Power Back Off) to base the transmit PSD of all lines on a reference line length so that the PSD at the receiving end is the same.

5.9.3 Rate Adaption

Rate adaption is the ability of a device to adjust from the configured transmission rate to the attainable transmission rate automatically depending on the line quality. The VDSL transmission rate then stays at the new rate or adjusts if line quality improves or deteriorates.

The VES determines line quality using the Signal-to-Noise Ratio (SNR). SNR is the ratio of the amplitude of the actual signal to the amplitude of noise signals at a given point in time. A low SNR indicates poor line quality.

Select **Fixed Rate** to disable transmission rate adjustment. If the attainable speeds cannot match configured speeds, then the VDSL link may go down or link communications may be sporadic due to line errors and consequent retransmissions

Select **Rate Adaptive Decrease Mode** to enable the VES to adjust to a new lower rate when the line quality deteriorates until the connection is broken. The VES will re-establish the line connection when the line quality improves. However, the new line rate might be lower that the configured line rate.

5.10VDSL Common Setup

To configure general VDSL port settings, click **Basic Setting** and **VDSL Common Setup** to display the screen as shown next.

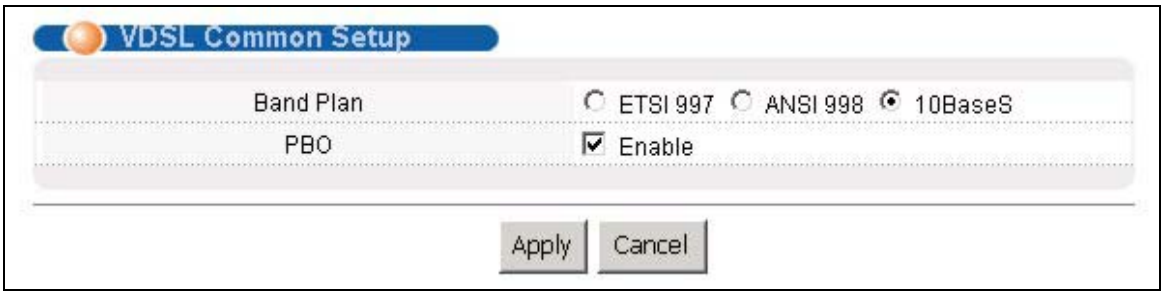


Figure 5-5 VDSL Common Setup

The following table describes the labels in this screen.

Table 5-6 VDSL Common Setup

LABEL	DESCRIPTION
Band Plan	Use the radio button to select a band plan.
PBO	PBO (Power Back Off) allows the switch to provide better service in a network environment with cables of varying lengths. Select **Enable** to activate this function.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.11VDSL Profile Setup

A profile is a table that contains a list of pre-configured VDSL settings. Each VDSL port has one (and only one) profile assigned to it at any given time. The profile defines VDSL parameters such as the payload rates. You can configure multiple profiles, including profiles for troubleshooting.

Profiles allow you to configure VDSL ports efficiently. You can configure all of the VDSL ports with the same profile, thus removing the need to configure the VDSL ports one-by-one. You can also change an individual VDSL port by assigning it a different profile.

For example, you could set up different profiles for different kinds of accounts (for example, economy, standard and premium). Assign the appropriate profile to a VDSL port and it takes care of a large part of the port's configuration.

To configure VDSL profiles, click **Basic Setting** and **VDSL Profile Setup** to display the screen as shown next

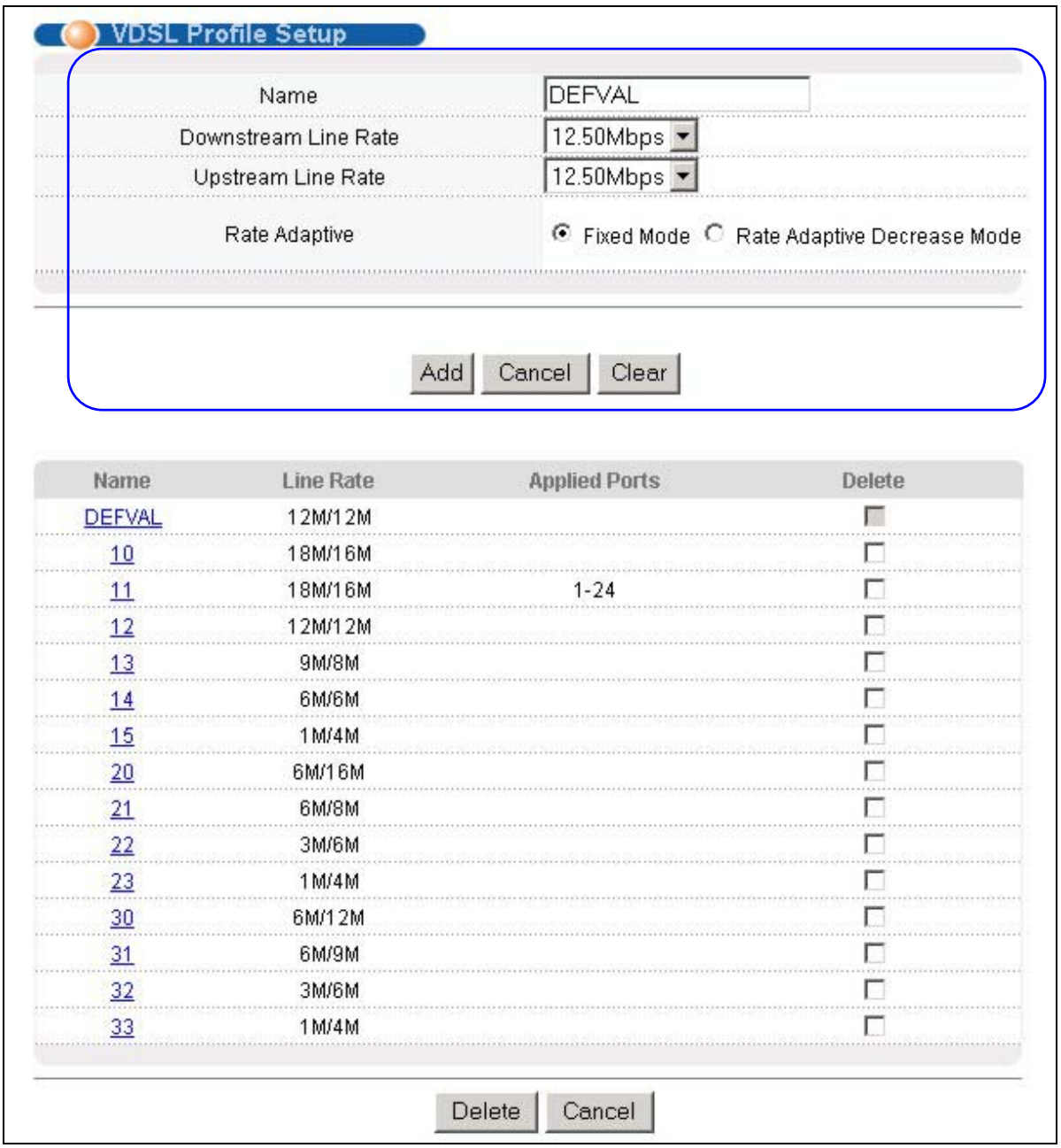


Figure 5-6 VDSL Profile Setup

The following table describes the labels in this screen.

Table 5-7 VDSL Profile Setup

LABEL	DESCRIPTION
Name	Enter a descriptive name for identification purposes.
Downstream Line Rate	Select the downstream line rate.
Upstream Line Rate	Select the upstream line rate.
Rate Adaptive	Select **Fixed Mode** or **Rate Adaptive Decrease Mode**. Refer to *section 5.9.3* for more information.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Delete	Click **Clear** to clear the fields to the factory defaults.

5.12Viewing and Editing VDSL Profiles

To view a summary of the profile configuration, scroll down to the summary table at the bottom of the **VDSL Profile Setup** screen.

To change the settings of a rule, click a number in the **Name** field.

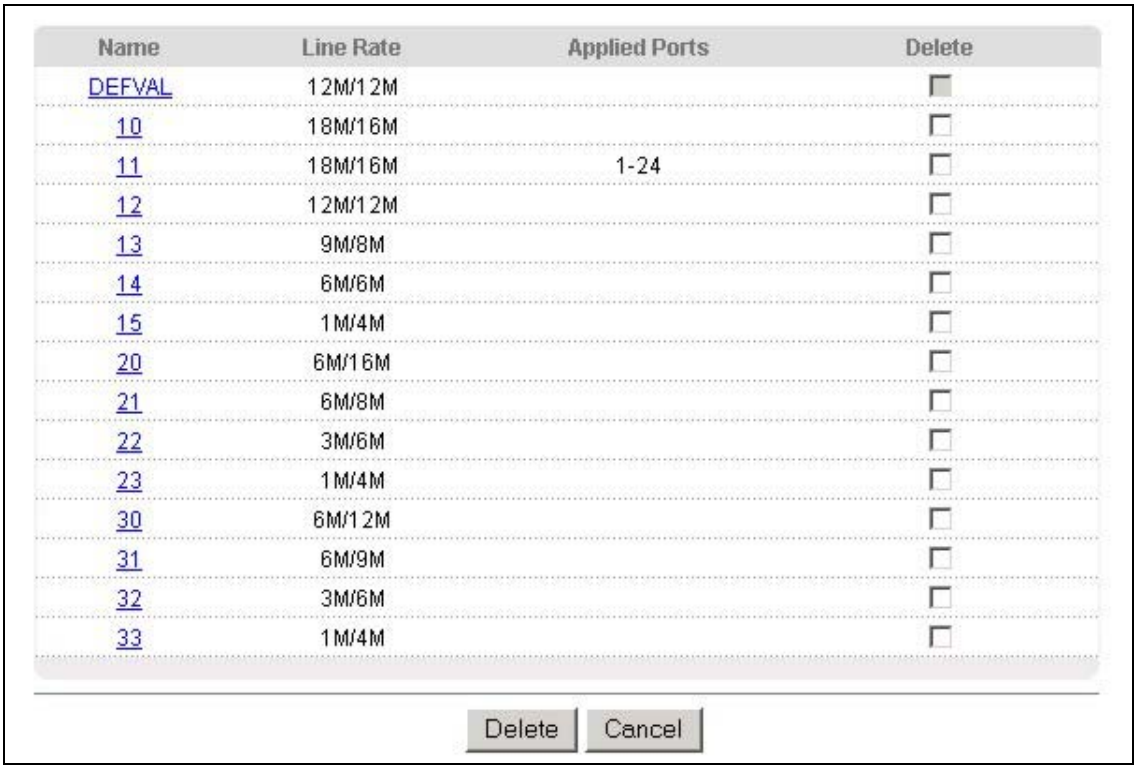


Figure 5-7 VDSL Profile Setup: Summary Table

The following table describes the labels in this screen.

Table 5-8 VDSL Profile Setup: Summary Table

LABEL	DESCRIPTION
Name	This field displays the descriptive name for this profile.
Line Rate	This field displays the configured maximum upstream and downstream line rates in megabits per second.
Applied Ports	This field displays the port ranges to which this profile is applied.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkboxes in the **Delete** column.

Part III:

Advanced Application 1

This part shows you how to configure the VLAN, Static MAC Forwarding, STP and Bandwidth Control Advanced Application screens.

Chapter 6 VLAN

*The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.*

6.1 Introduction to IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 (212) VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

The VES handles up to 4094 VLANs (VIDs 1-4094). The switch accepts incoming frames with VIDs 1-4094.

6.1.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

6.1.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

Please refer to the following table for common GARP terminology.

Table 6-1 GARP Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

6.2 802.1Q VLAN

Follow the steps below to set the **802.1Q VLAN Type** on the switch.

1. Select **802.1Q** as the **VLAN Type** in the **Switch Setup** screen (under **Basic Setting**) and click **Apply**.

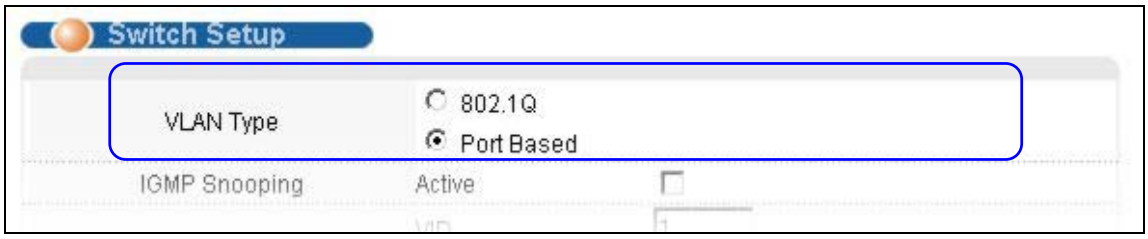


Figure 6-1 Selecting a VLAN Type

2. Click **VLAN** under **Advanced Application** to display the **VLAN Status** screen as shown next.

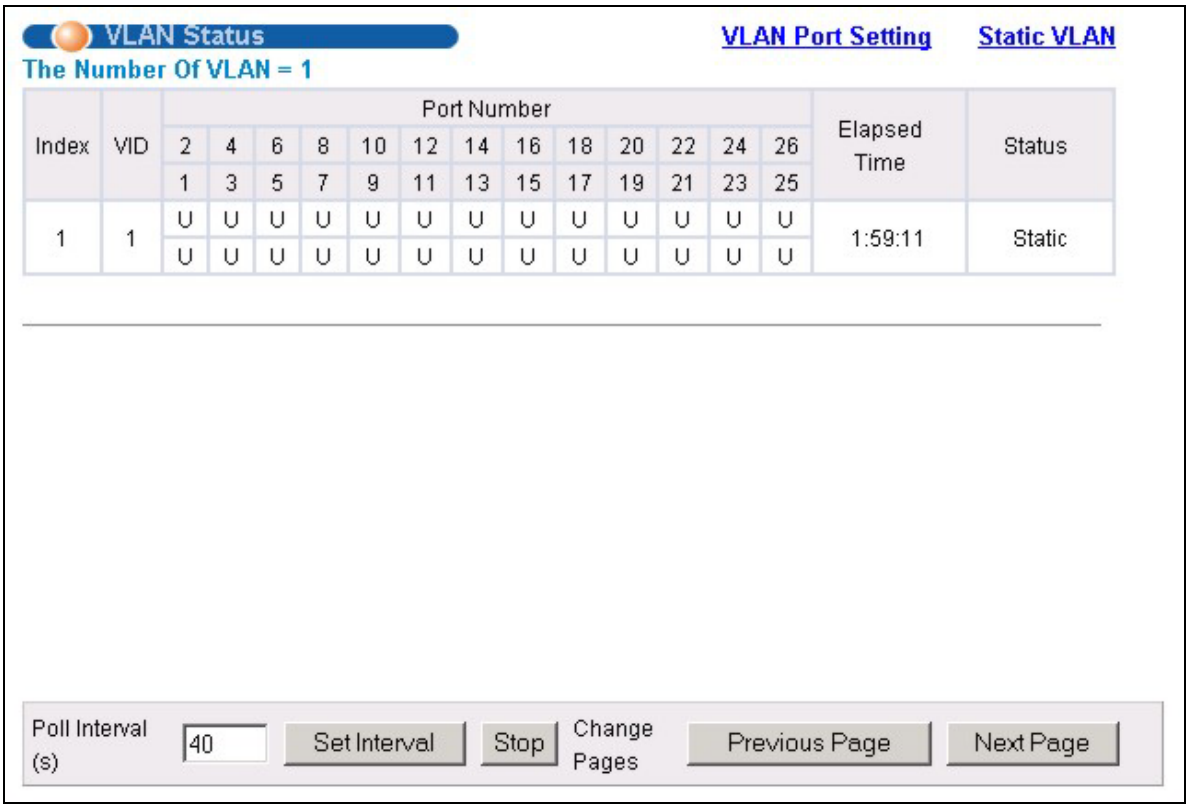


Figure 6-2 802.1Q VLAN Status

The following table describes the labels in this screen.

Table 6-2 802.1Q VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the switch.

Table 6-2 802.1Q VLAN Status

LABEL	DESCRIPTION
Index	This is the VLAN index number.
VID	VID is the PVID, the Port VLAN ID assigned to untagged frames or priority-tagged frames received on this port that you configure in the **VLAN Port Setting** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN in marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamically using GVRP or statically, that is, added as a permanent entry.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.
Previous/Next Page	Click one of these buttons to show the previous/next screen if all status information cannot be seen in one screen.

6.2.1 802.1Q VLAN Port Settings

To configure the 802.1Q VLAN settings on a port, click the **VLAN Port Setting** link in the **VLAN Status** screen.

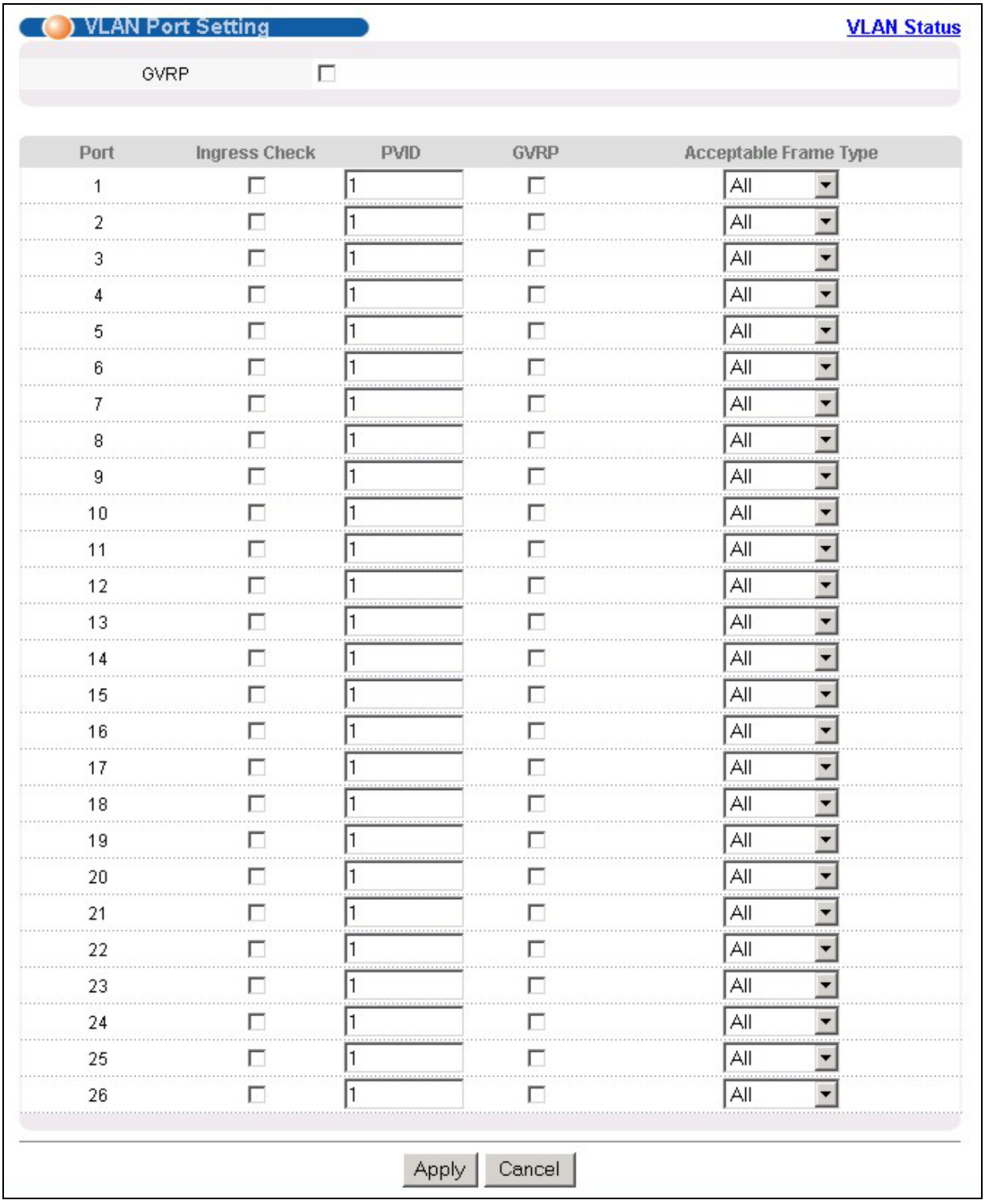


Figure 6-3 802.1Q VLAN Port Settings

The following table describes the labels in this screen.

Table 6-3 802.1Q VLAN Port Settings

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to dynamically register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local switch.
Port	This field displays the port numbers.
Ingress Check	If this check box is selected for a port, the device discards incoming frames for VLANs that do not include this port in its member set.
PVID	Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the default ingress port's VLAN ID, the PVID. The default PVID is VLAN 1 for all ports, but this can be changed to any number between 1 and 4094.
GVRP	Select this check box to permit VLANs groups beyond the local switch on this port. GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All** and **Tag Only**. Select **All** to accept all frames with untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames are dropped.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring the screen again.

6.2.2 802.1Q Static VLAN

You can dynamically have a port join a VLAN group using GVRP, permanently assign a port to be a member of a VLAN group or prohibit a port from joining a VLAN group in this screen. Click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

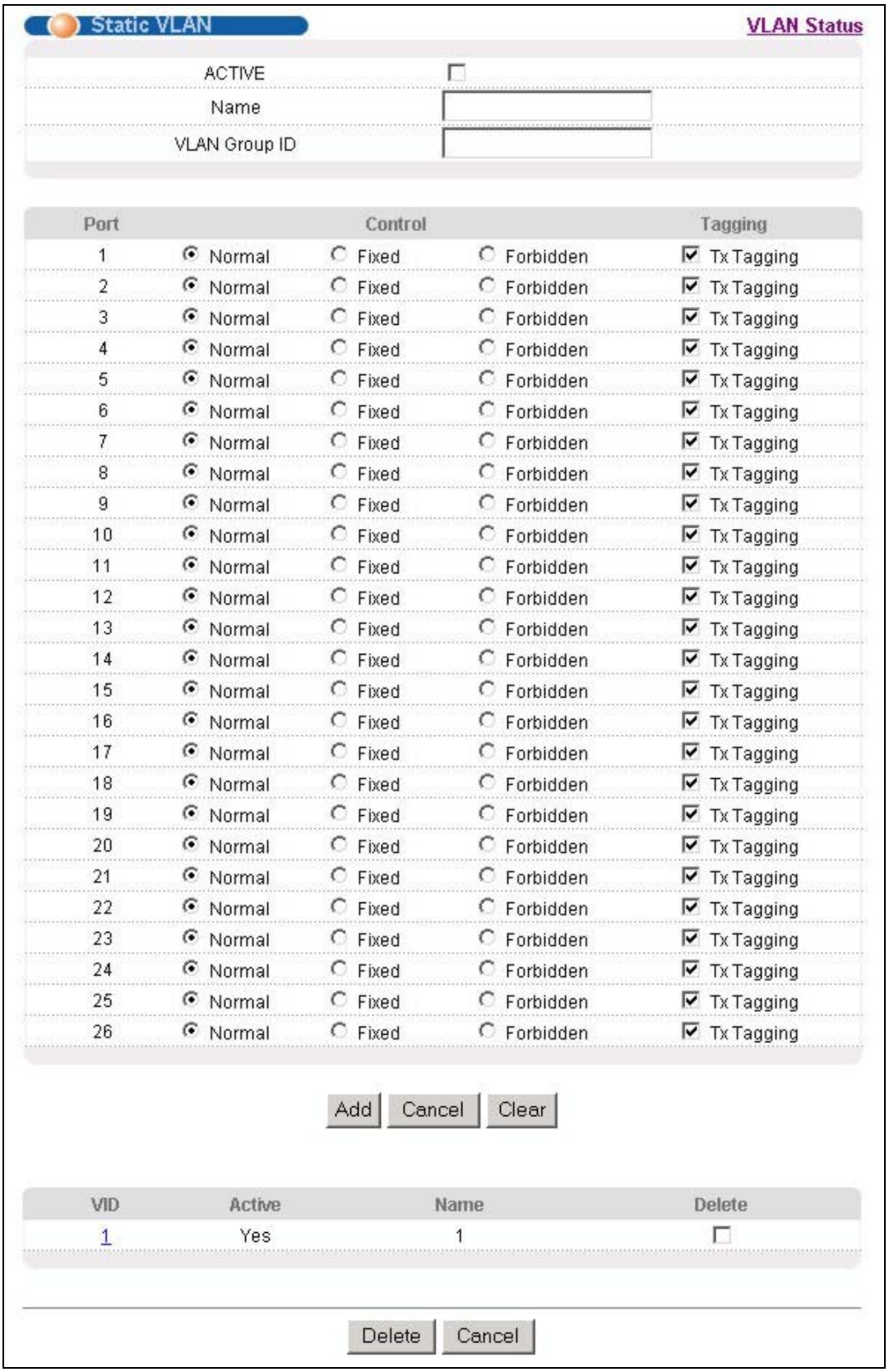


Figure 6-4 802.1Q Static VLAN

The following table describes the labels in this screen.

Table 6-4 802.1Q Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to enable the VLAN.
Name	Enter a descriptive name for this VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static VLAN entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.

6.2.3 Viewing and Editing VLAN Settings

To view a summary of the VLAN configuration, scroll down to the summary table at the bottom of the **Static VLAN** screen.

To change the settings of a rule, click a number in the **VID** field.

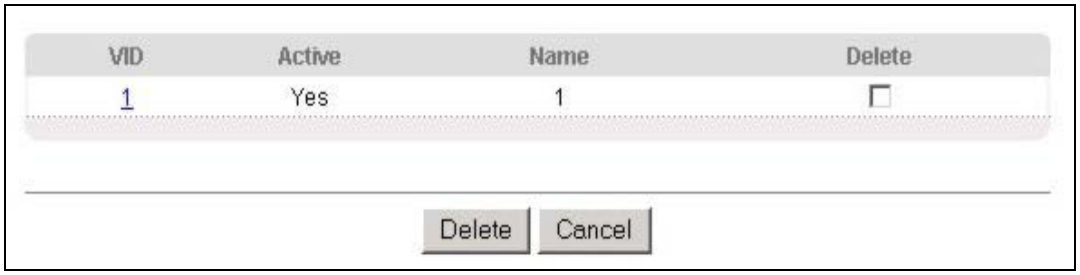


Figure 6-5 Static VLAN: Summary Table

The following table describes the labels in this screen.

Table 6-5 Static VLAN: Summary Table

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

VID1 Example Screen

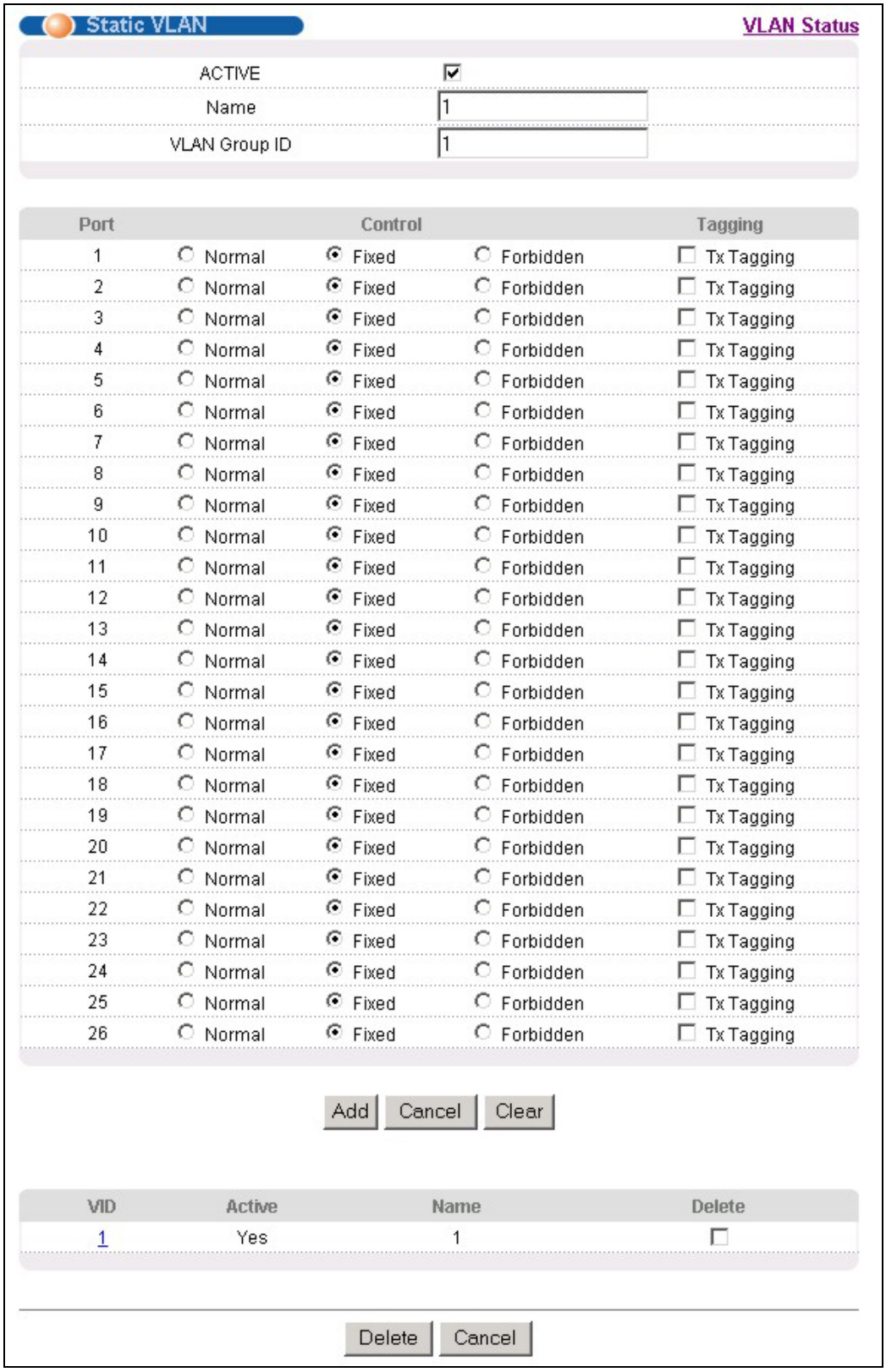


Figure 6-6 VID1 Example Screen

6.3 Introduction to Port-based VLANs

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

6.3.1 Configuring a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen under **Basic Setting** and then click **VLAN** under **Advanced Application** to display the next screen.

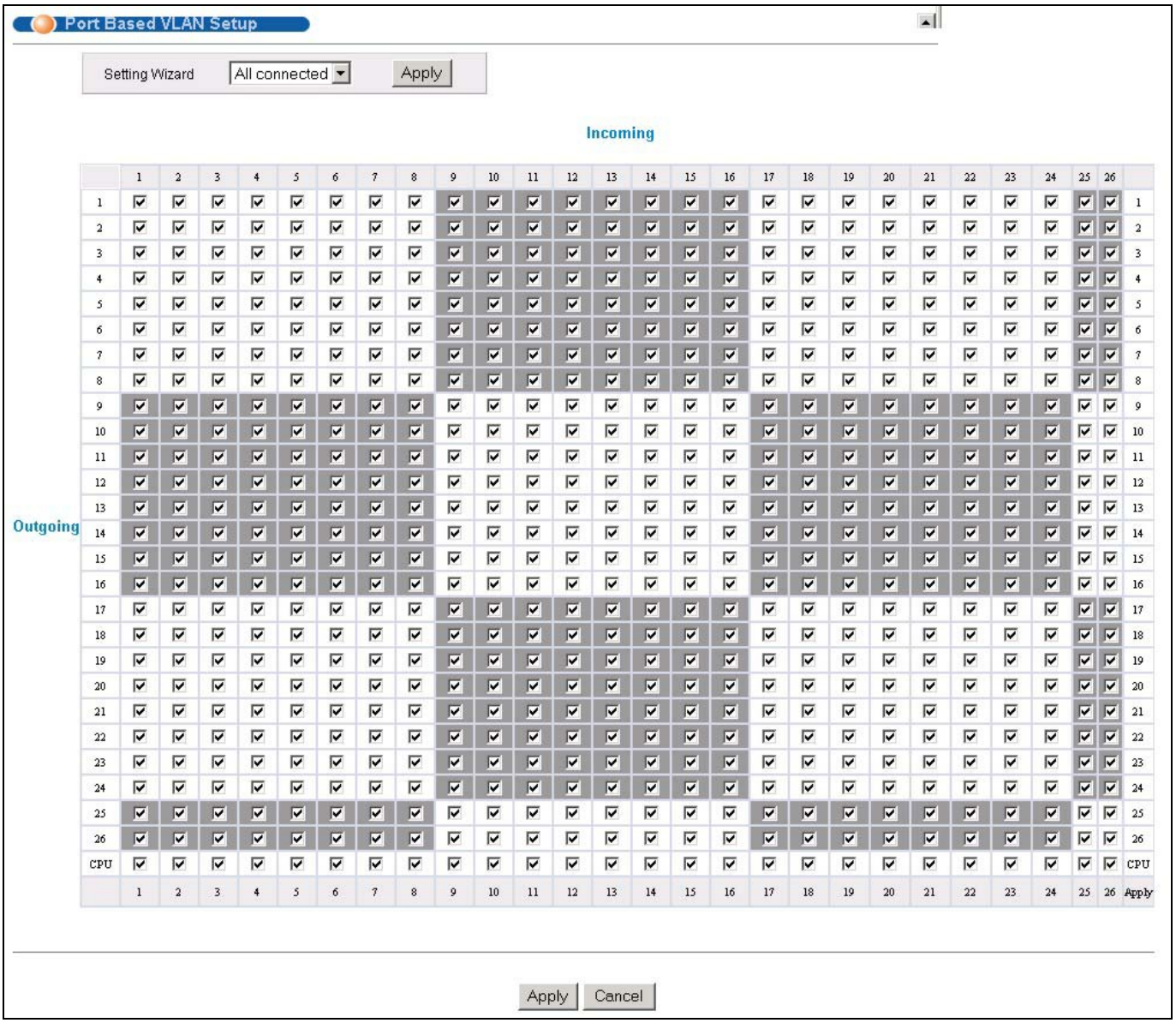

Port Based VLAN Setup
Setting Wizard
All connected
Apply
Incoming
Outgoing
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
CPU
Apply
Cancel

Figure 6-7 Port Based VLAN Setup (All Connected)

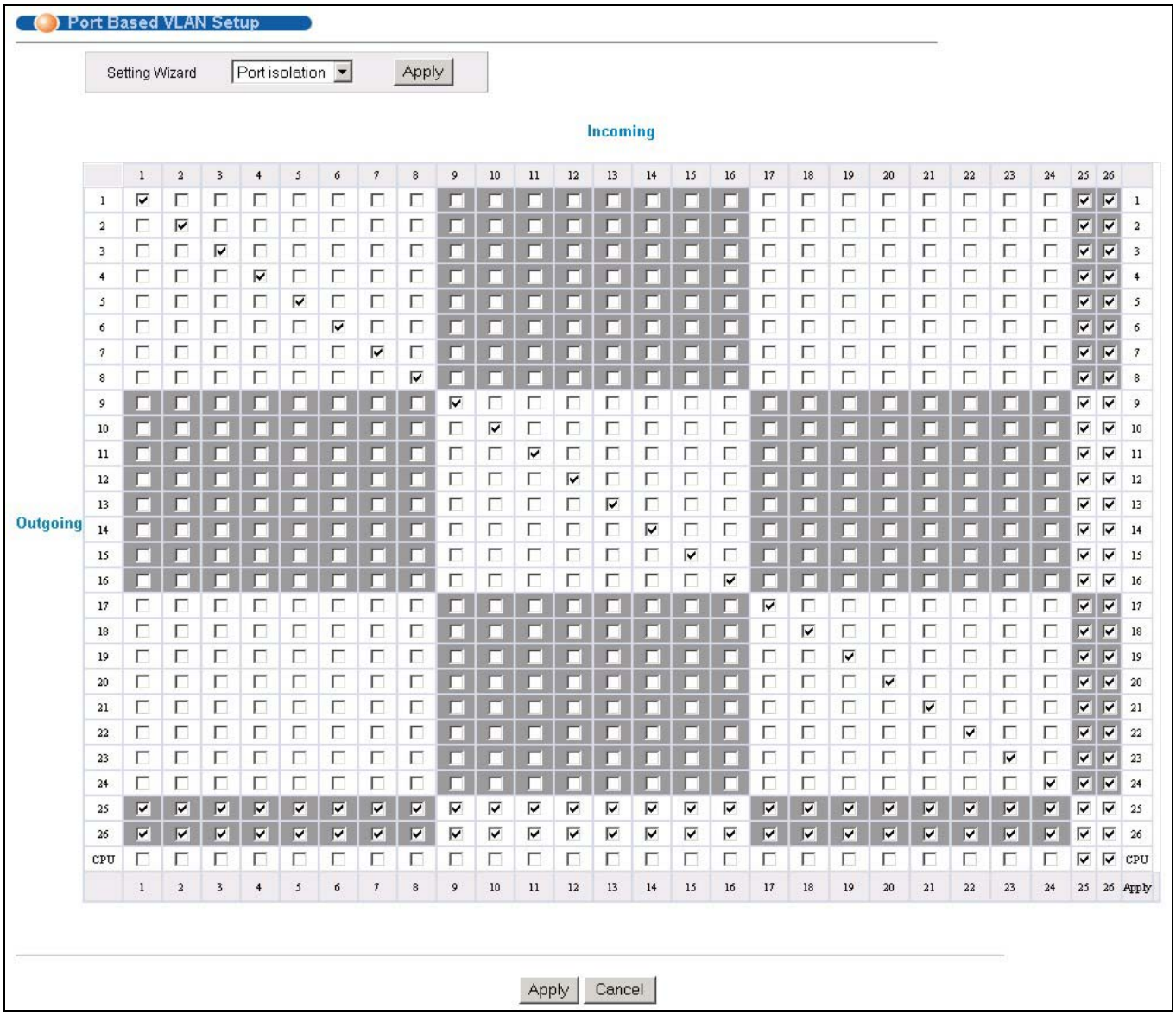


Figure 6-8 Port Based VLAN Setup (Port Isolation)

The following table describes the labels in this screen.

Table 6-6 Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose from **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected (*Figure 6-7*). This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the Ethernet port (port 25) and cannot communicate with each other or the CPU management port (see *Figure 6-8*). This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.

Table 6-6 Port Based VLAN Setup

LABEL	DESCRIPTION
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the switch management port. By default it forms a VLAN with all ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the switch management port. By default it forms a VLAN with all ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Apply	Click **Apply** to save the changes, including the "wizard settings".
Cancel	Click **Cancel** to start configuring the screen again.

Chapter 7
Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

7.1 Introduction to Static MAC Forward Setup

A static MAC address entry is an address that has been manually entered in the MAC address learning table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. Devices that match static MAC address rules on a port can *only* receive traffic on that port and cannot receive traffic on other ports. This may reduce unicast flooding.

7.2 Configuring Static MAC Forwarding

Click **Static MAC Forwarding** to display the configuration screen as shown.

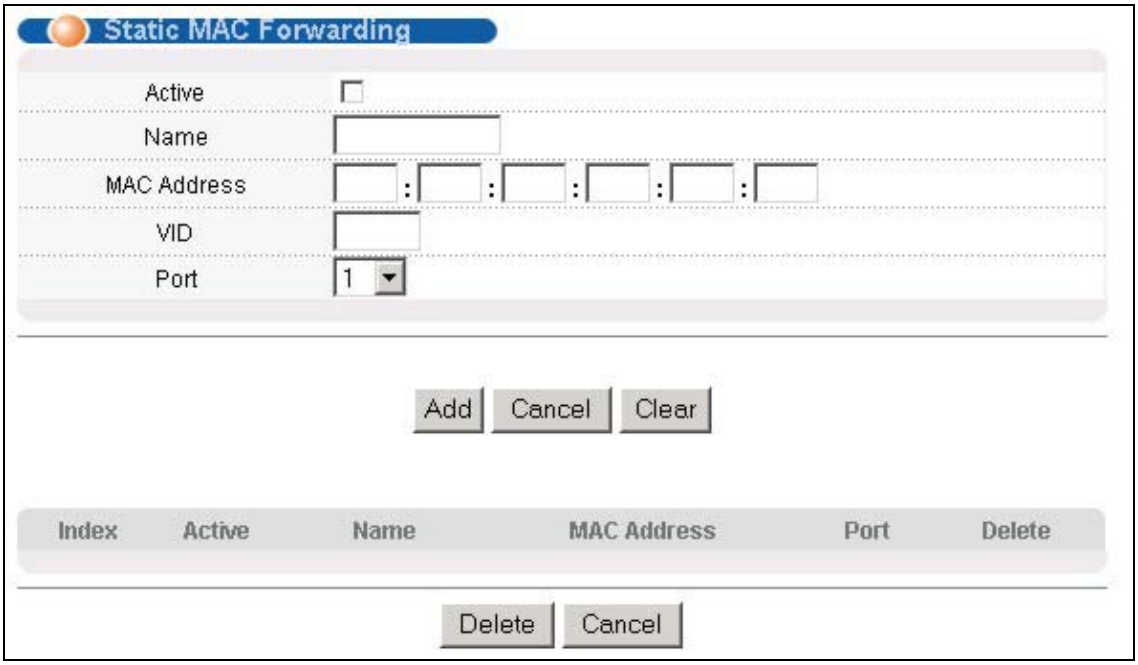


Figure 7-1 Static MAC Forwarding

The following table describes the labels in this screen.

Table 7-1 Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.

Table 7-1 Static MAC Forwarding

LABEL	DESCRIPTION
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded. Select **filter** to filter the destination MAC address entered in the previous field. This means that the switch drops all packets destined for that MAC address on all ports.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.

7.3 Viewing and Editing Static MAC Forwarding Rules

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Static MAC Forwarding** screen.

To change the settings of a rule, click a number in the **Index** field.

Figure 7-2 Static MAC Forwarding: Summary Table

The following table describes the labels in this screen.

Table 7-2 Static MAC Forwarding: Summary Table

LABEL	DESCRIPTION
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
Port	This field displays the port where the MAC address shown in the **MAC Address** field will be forwarded. This field displays **filter** when the switch is set to drop packets destined for the MAC address shown in the **MAC Address** field on all ports.
Delete	Check the rule(s) that you want to remove in the **Delete** column, and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkboxes in the **Delete** column.

Chapter 8
Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP).

8.1 Introduction to Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other STP-compliant switches in your network to ensure that only one route exists between any two stations on the network.

8.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

Table 8-1 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

8.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

8.3.1 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 8-2 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

8.4 STP Status

Click **Advanced Application** and then **Spanning Tree Protocol** in the navigation panel to display the STP status as shown in the screen next.

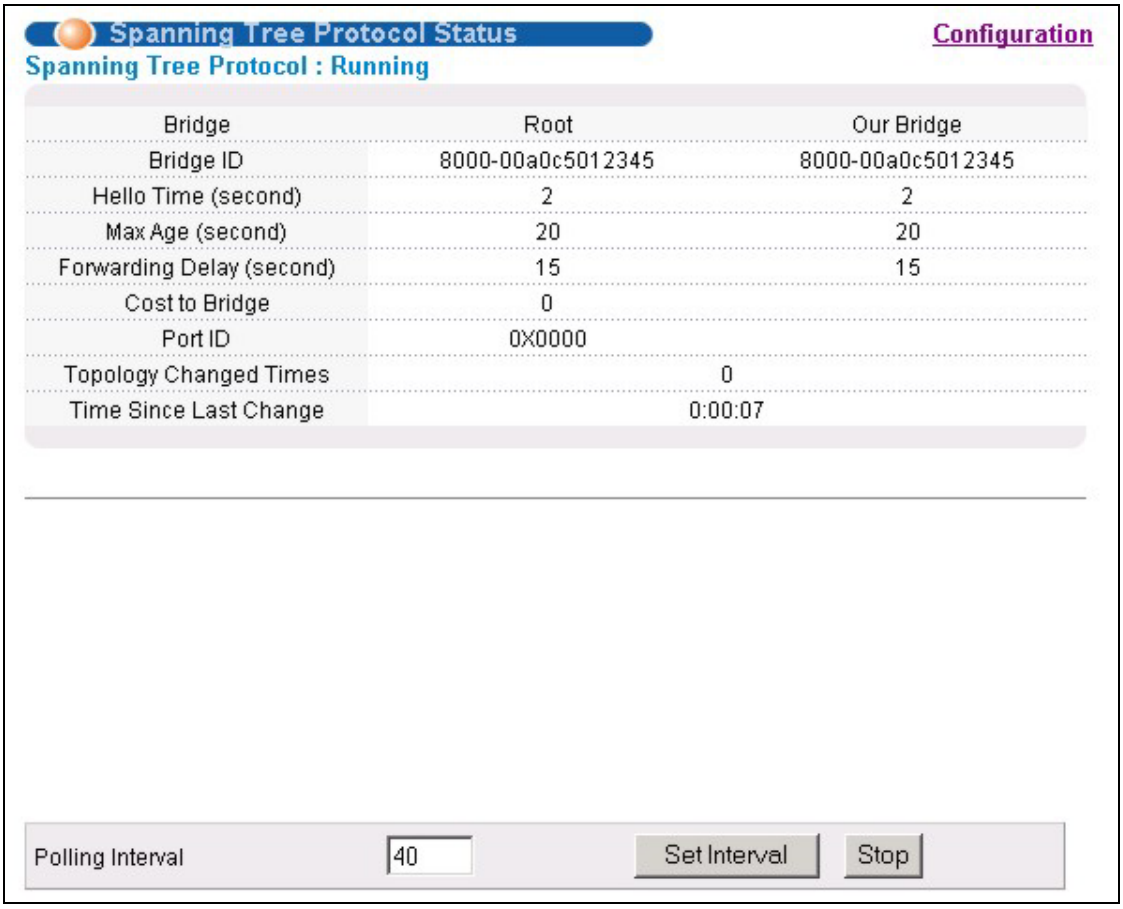


Figure 8-1 Spanning Tree Protocol: Status

The following table describes the labels in this screen.

Table 8-3 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Spanning Tree Protocol	This field displays **Running** if STP is activated. Otherwise, it displays **Down**.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time, Max Age** and **Forwarding Delay**
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.

Table 8-3 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt STP statistic polling.

8.4.1 Configuring STP

To configure STP, click the **Configuration** link in the **Spanning Tree Protocol** screen as shown next.

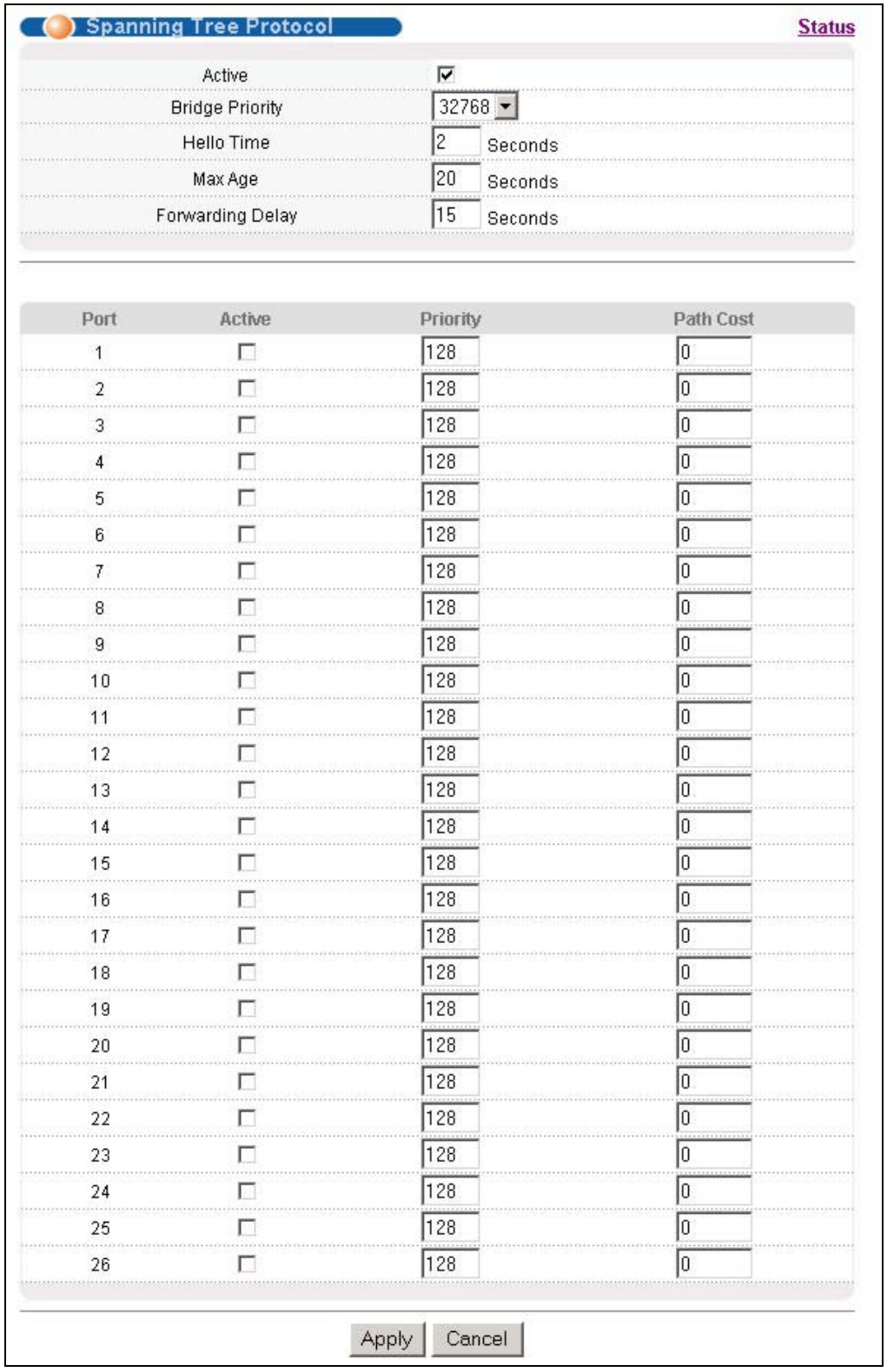


Figure 8-2 Spanning Tree Protocol: Configuration

The following table describes the labels in this screen.

Table 8-4 Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Active	Select this check box to activate STP.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. The allowed range is 0 to 61440. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: **2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)**
Port	This field displays the port number.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see *Table 8-1* for more information.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 9
Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth allowed from specific source(s) to specified destination(s) using the Bandwidth Control setup screens.

9.1 Introduction to Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for traffic flows going into or going out from individual VDSL ports. Click **Advanced Application** and then **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

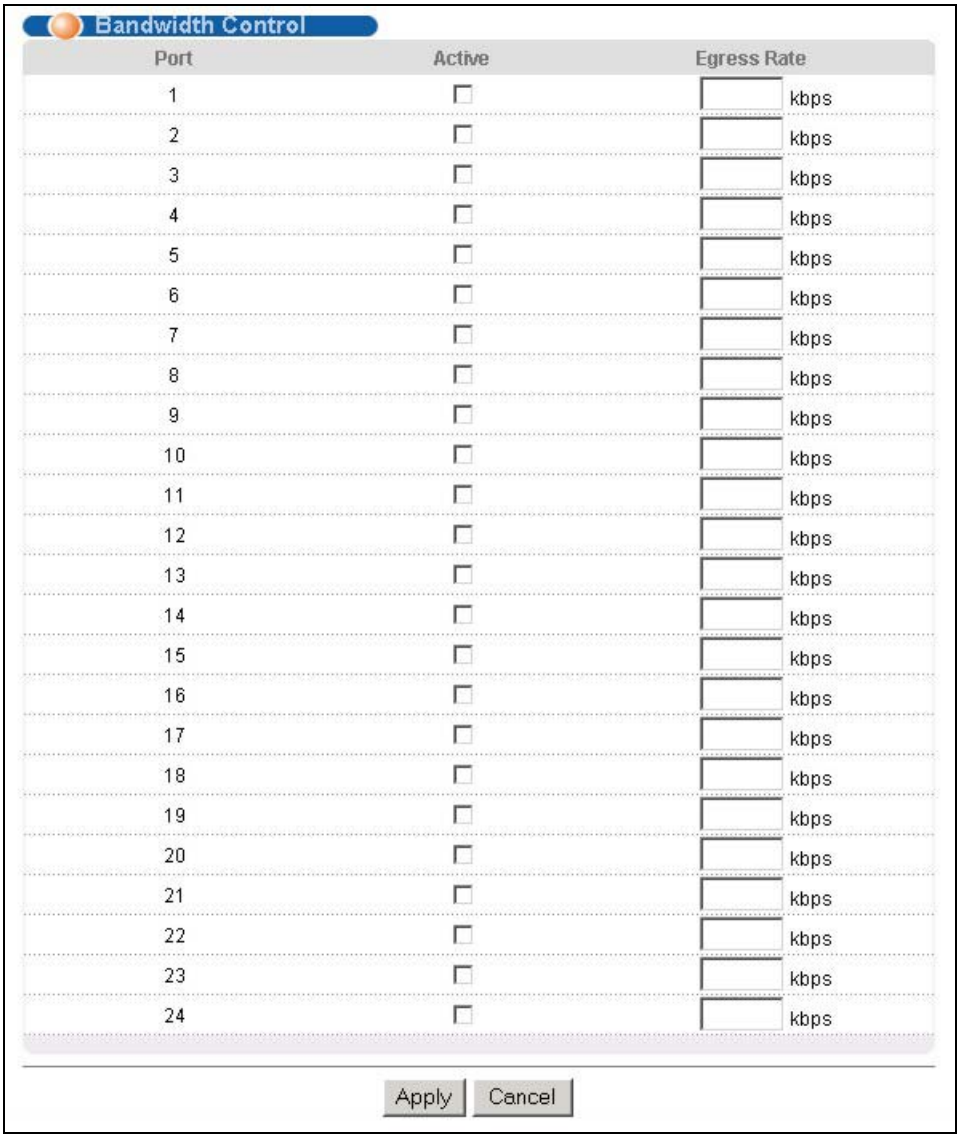


Figure 9-1 Bandwidth Control

The following table describes the labels in this screen.

Table 9-1 Bandwidth Control

LABEL	DESCRIPTION
Port	This field displays the port number.
Active	Select this check box to enable bandwidth control on a VDSL port. Clear this check box to disable bandwidth control on a VDSL port.
Egress Rate	Type the maximum bandwidth allowed in kilobits per second (kbps) for traffic going out of this port. Enter a number between 100 and 100000.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

Part IV:

Advanced Application 2

This part shows you how to configure the Broadcast Storm Control, Mirroring, Link Aggregation, Port Authentication, Port Security, Access Control and Queuing Method Advanced Application screens.

Chapter 10
Broadcast Storm Control

*This chapter discusses the **Broadcast Storm Control** screen.*

10.1 Introducing Broadcast Storm Control

Broadcast storm control limits the percentage of broadcast frames that can be stored in the switch buffer or sent out from the switch. The switch discards broadcast frames that exceed the threshold percentage. Enable this feature to reduce broadcast traffic coming into your network.

10.2 Configuring Broadcast Storm Control

Click **Broadcast Strom Control** in the navigation panel to display the screen as shown next.

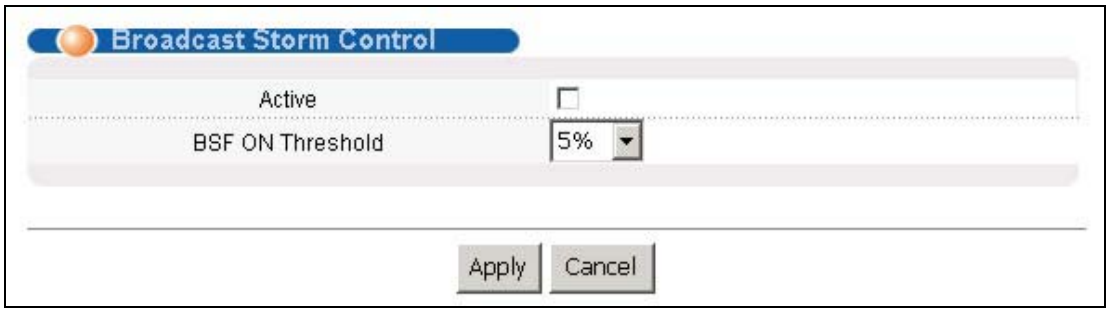


Figure 10-1 Broadcast Storm Control

The following table describes the labels in this screen.

Table 10-1 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control on the switch.
BSF ON Threshold	Use the drop-down list box to select the Broadcast Storm Filtering (BSF) threshold. The switch starts discarding broadcast frames when the percentage of broadcast frames (out of total frames) exceeds this threshold. The switch discards broadcast frames until the percentage falls back below the threshold.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 11 Mirroring

*This chapter discusses the **Mirroring** screen.*

11.1 Introduction to Port Mirroring

Port mirroring allows you to copy traffic from mirrored ports to a monitor port so you can examine the traffic on the monitor port without interfering with the traffic on the mirrored ports.

11.2 Port Mirroring Configuration

Click **Advanced Application** and then **Mirroring** in the navigation panel to display the **Mirroring** screen.

11.2.1 Setting Up Port Mirroring

You must first select a monitor port. A monitor port is a port that copies the traffic of mirrored ports.

Figure 11-1 Mirroring

The following table describes the related labels in this screen.

Table 11-1 Mirroring

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Monitor Port	The monitor port is the port to which you copy the traffic from mirrored ports. Do this to examine the mirrored ports' traffic in more detail without interfering with the traffic flow on the mirrored port(s). Select a monitor port from this drop-down list box.
Direction	Select which direction of traffic you want to copy from the mirrored port(s) to the monitor port. Select **Ingress** to copy the traffic coming into the switch through the mirrored port(s). Select **Egress** to copy the traffic going out of the switch through the mirrored port(s). Select **Both** to copy the traffic coming into or going out of the switch through the mirrored port(s).
Port	A mirrored port is a port from which you copy the traffic to the monitor port. Do this to examine the mirrored port's traffic in more detail without interfering with the traffic flow on the mirrored port. Select the **Mirrored** check box for each port from which you want to copy traffic. You can select more than one mirrored port.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring the screen again.

Chapter 12 Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

12.1 Introduction to Link Aggregation

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A link aggregation group is one logical link containing multiple ports.

12.1.1 Dynamic Link Aggregation

The VES adheres to the 802.3ad standard for static and dynamic (LACP) port trunking.

The VES supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention

Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

12.1.2 Link Aggregation ID

LACP aggregation ID consists of the following information:

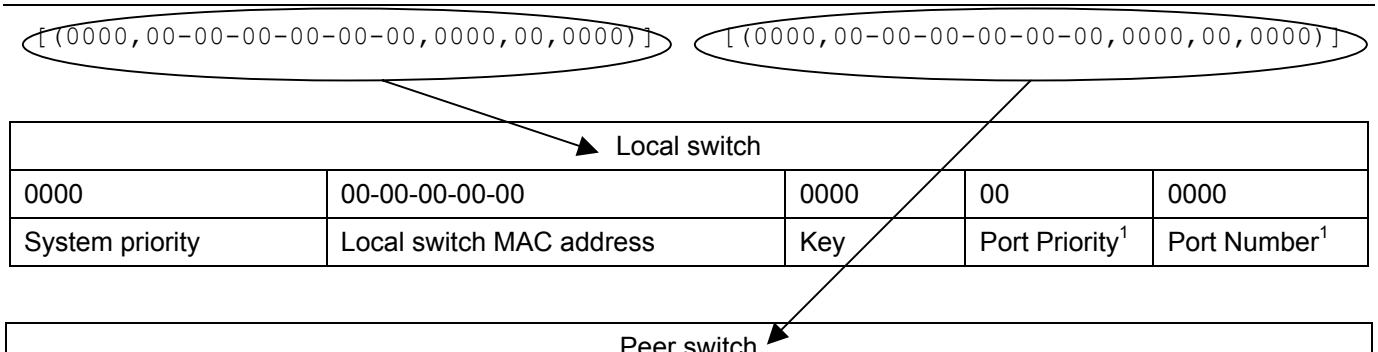


Figure 12-1 Aggregation ID

12.2 Link Aggregation Protocol Status

Click **Advanced Application**, **Link Aggregation** in the navigation panel to display the **Link Aggregation Protocol Status** screen.

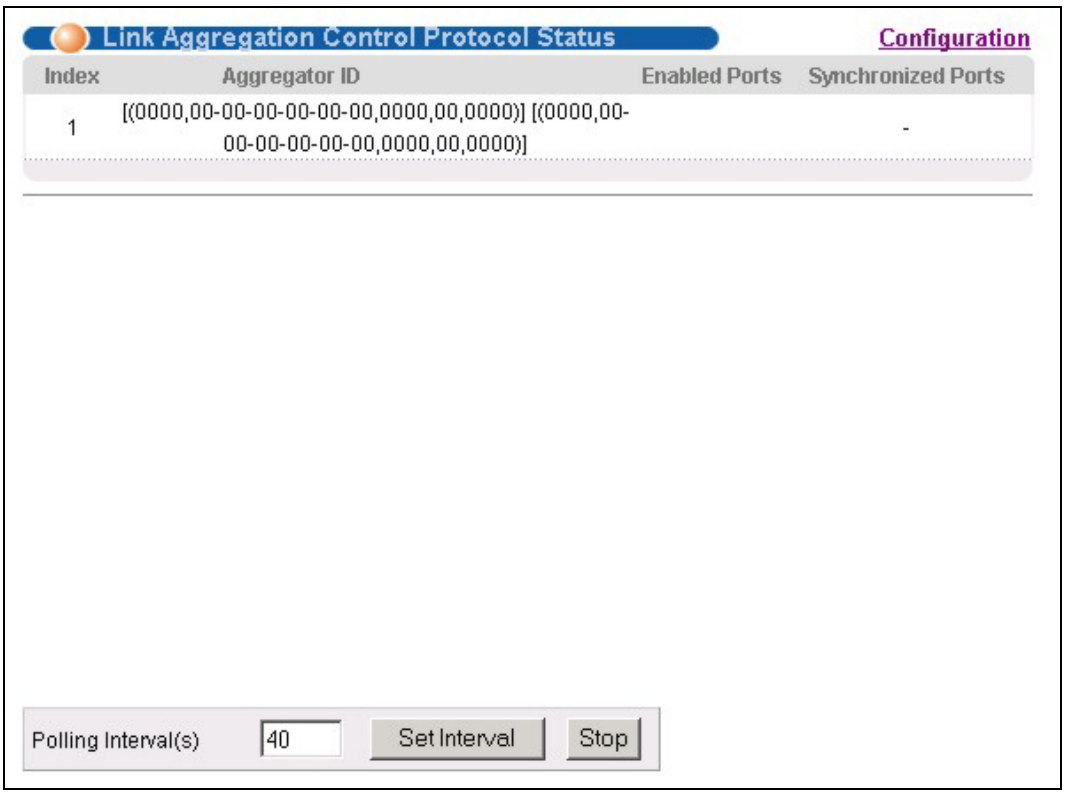


Figure 12-2 Link Aggregation: Link Aggregation Protocol Status

The following table describes the labels in this screen.

[1] This is "0" as it is the aggregator ID for the link aggregation group, not the individual port.

Table 12-1 Link Aggregation: Link Aggregation Protocol Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	Refer to *Figure 12-1* for more information on this field.
Enabled Port	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

12.3Link Aggregation Setup

Click **Configuration** in the **Link Aggregation Protocol Status** screen to display the screen shown next.

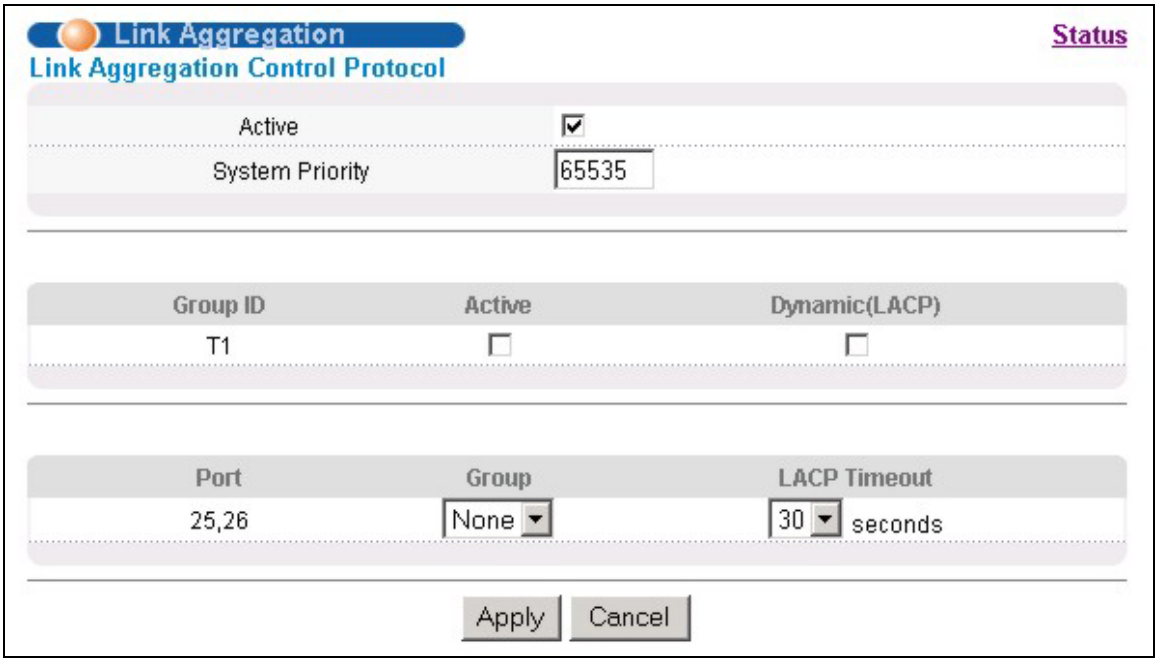


Figure 12-3 Link Aggregation: Configuration

The following table describes the labels in this screen.

Table 12-2 Link Aggregation: Configuration

LABEL	DESCRIPTION
Link Aggregation Control Protocol	

Table 12-2 Link Aggregation: Configuration

LABEL	DESCRIPTION
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,355. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	This field identifies the trunk group, that is, one logical link containing multiple ports.
Active	Make sure to select this check box to activate the trunk group. You may temporarily deactivate a trunk group without deleting it by clearing this check box.
Dynamic LACP	Select this check box to enable LACP for a trunk group.
Port	This is the ports in the trunk group's port range and is not configurable.
Group	Select **T1** to add the ports to the link aggregation group. Otherwise, select **None** to remove the ports from the group.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 13
Port Authentication

This chapter describes the 802.1x authentication method and RADIUS server connection setup.

13.1 Introduction to Authentication

IEEE 802.1x is an extended authentication protocol2 that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

13.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

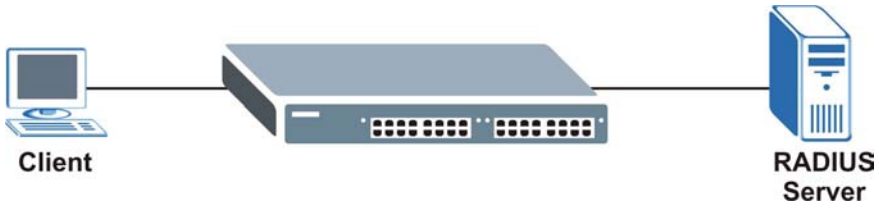


Figure 13-1 RADIUS Server

13.2 Configuring Port Authentication

To enable port authentication, first activate IEEE802.1x security (both on the switch and the port(s)) then configure the RADIUS server settings.

Click **Port Authentication** under **Advanced Application** in the navigation panel to display the screen as shown.

2 At the time of writing, Windows XP of the Microsoft operating systems supports 802.1x. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

Figure 13-2 Port Authentication

13.2.1 Configuring RADIUS Server Settings

From the **Port Authentication** screen, click **RADIUS** to display the configuration screen as shown.

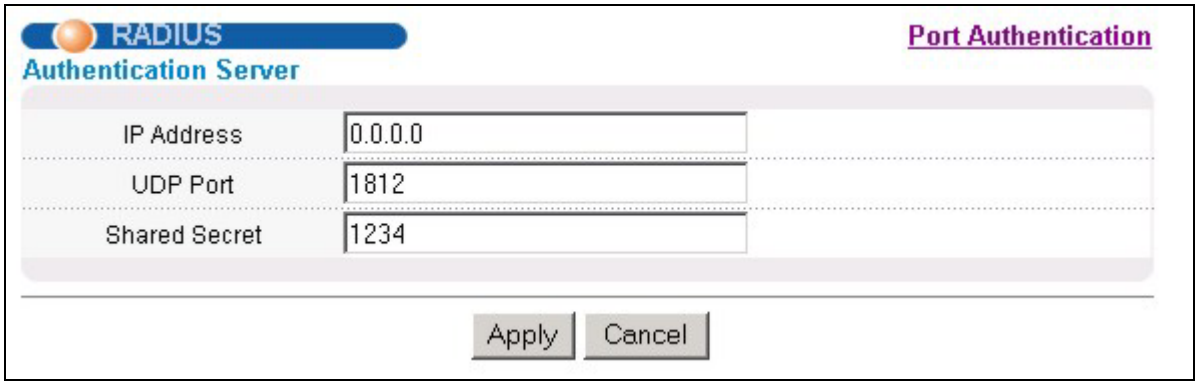


Figure 13-3 Port Authentication: RADIUS

The following table describes the labels in this screen.

Table 13-1 Port Authentication: RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.2.2 Configuring IEEE802.1x

From the **Port Authentication** screen, click **802.1x** to display the configuration screen as shown.

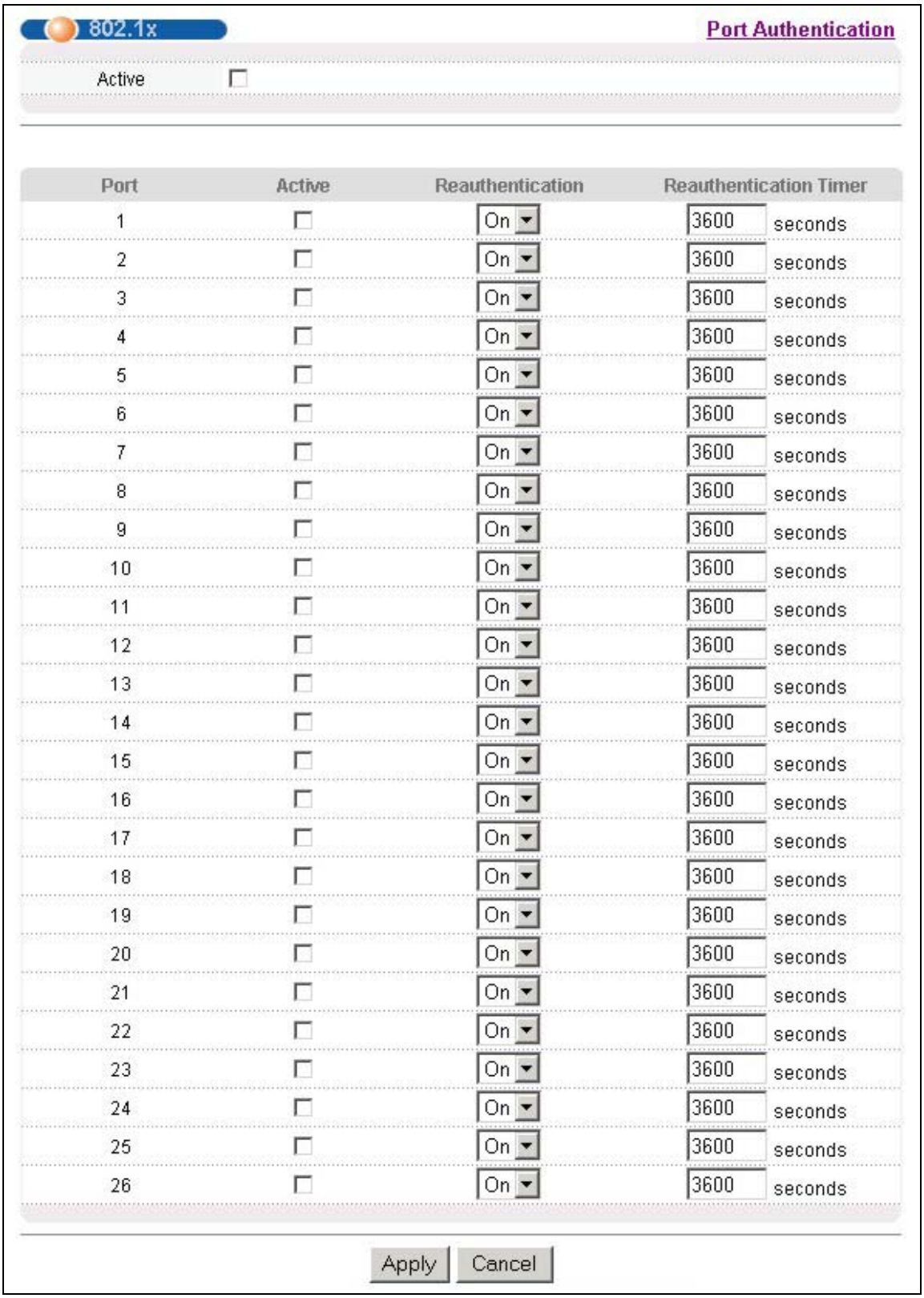


Figure 13-4 Port Authentication: 802.1x

The following table describes the labels in this screen.

Table 13-2 Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch.
	You must first allow 802.1x authentication on the switch before configuring it on each port.
Port	This field displays a port number.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 14
Port Security

This chapter shows you how to set up port security.

14.1 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch. The switch can learn up to MAC addresses in total with no limit on individual ports other than the sum cannot exceed

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable **Port Security** together with MAC address learning as this will result in many broadcasts

14.2 Port Security Setup

Click **Port Security** in the navigation panel to display the screen as shown.

Figure 14-1 Port Security

The following table describes the labels in this screen.

Table 14-1 Port Security

LABEL	DESCRIPTION
Port	This field displays a port number.
Active	Select this check box to have this port only accept frames from static MAC addresses that are configured for the port. The switch will drop frames from MAC addresses that are not statically configured for the port.
Apply	Click **Apply** to save your changes back to the switch.

Table 14-1 Port Security

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 15 Access Control

This chapter describes how to control access to the switch.

15.1 About Access Control

Click **Advanced Application**, **Access Control** from the navigation panel to display the screen as shown. From this screen you can configure SNMP, up to four web configurator administrators, enable/disable remote service access and configure trusted computers for remote access.

Figure 15-1 Access Control

15.2 Access Control Overview

A console port access control session and Telnet access control session cannot coexist. The console port has higher priority. If you telnet to the switch and someone is already logged in from the console port, then you will see the following message.

```
"Local administrator is configuring this device now!!!
Connection to host lost."
```

Figure 15-2 Console Port Priority

A console port or Telnet session can coexist with one FTP session, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions.

Table 15-1 Access Control Summary

	Console port	Telnet	FTP	Web	SNMP
Number of sessions allowed	1	1	1	5	No limit
Number of concurrent sessions allowed	1 console port or Telnet. Console port has priority.		1	5	No limit

15.3 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network switches. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the VES through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

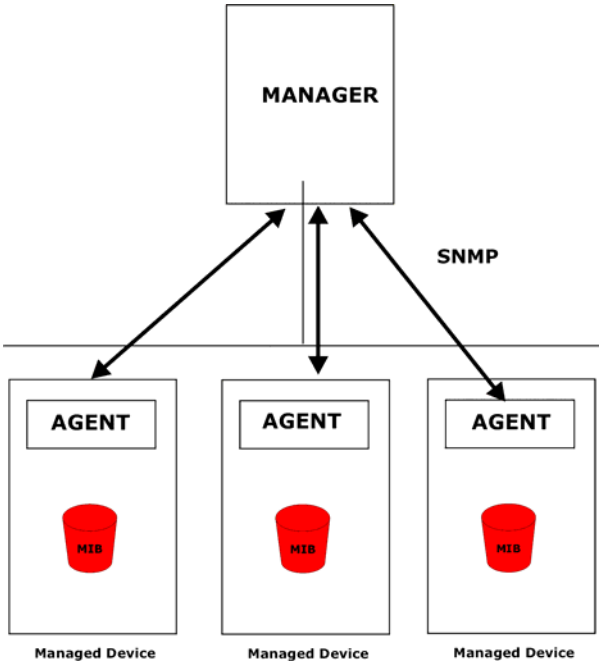


Figure 15-3 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the VES). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 15-2 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

Table 15-2 SNMP Commands

COMMAND	DESCRIPTION
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

15.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The VES supports the following MIBs:

- SNMP MIB II (RFC1213)
- RFC1493 Bridge MIBs
- RFC1643 Ethernet MIB
- RFC1757 RMON
- RFC1155 SNMP v1
- RFC2647 Bridge MIB extension (for 802.1Q)
- VDSL private MIB

15.3.2 SNMP Traps

The VES sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 15-3 SNMP Traps

GENERIC TRAP	SPECIFIC TRAP	DESCRIPTION
0 (Cold Start)	0	This trap is sent when the VES is turned on.
1 (WarmStart)	0	This trap is sent when the VES restarts.
2 (linkDown)	0	This trap is sent when the Ethernet link is down.
3 (linkUp)	0	This trap is sent when the Ethernet link is up.
4 (authenticationFailure)	0	This trap is sent when an SNMP request comes from non-authenticated hosts.

15.3.3 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

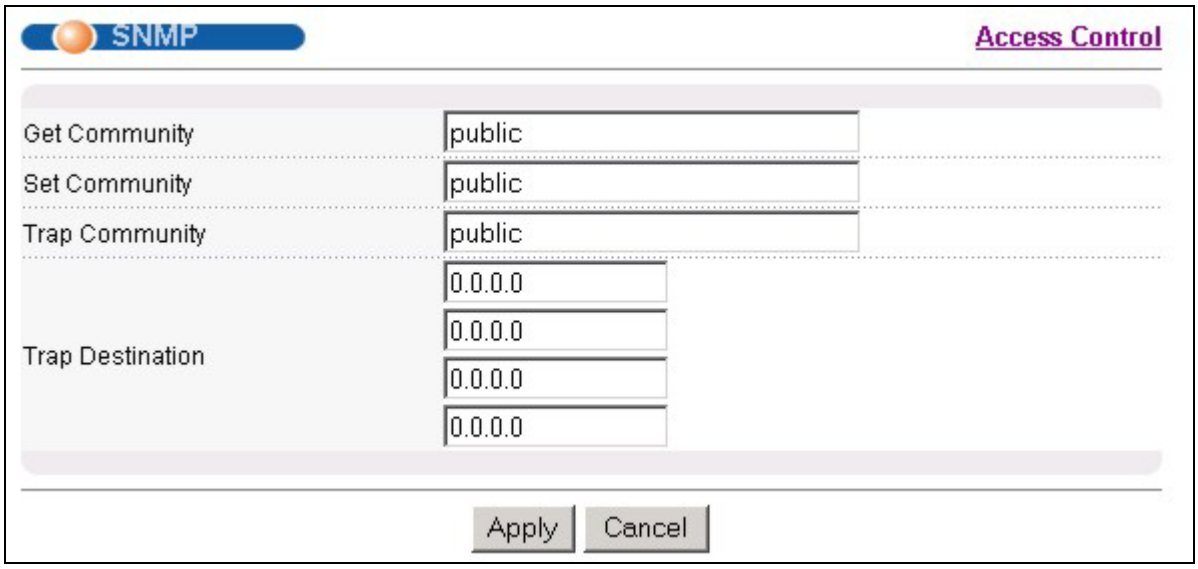


Figure 15-4 Access Control: SNMP

The following table describes the labels in this screen.

Table 15-4 Access Control: SNMP

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext-requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap: Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap: Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.3.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the VES via web configurator at any one time.

1. An administrator is someone who can both view and configure VES changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

It is highly recommended that you change the default administrator password ("1234").

2. A non-administrator (username is something other than **admin**) is someone who can view but not configure VES changes.

Click **Access Control** from the navigation panel and then click Logins from this screen.

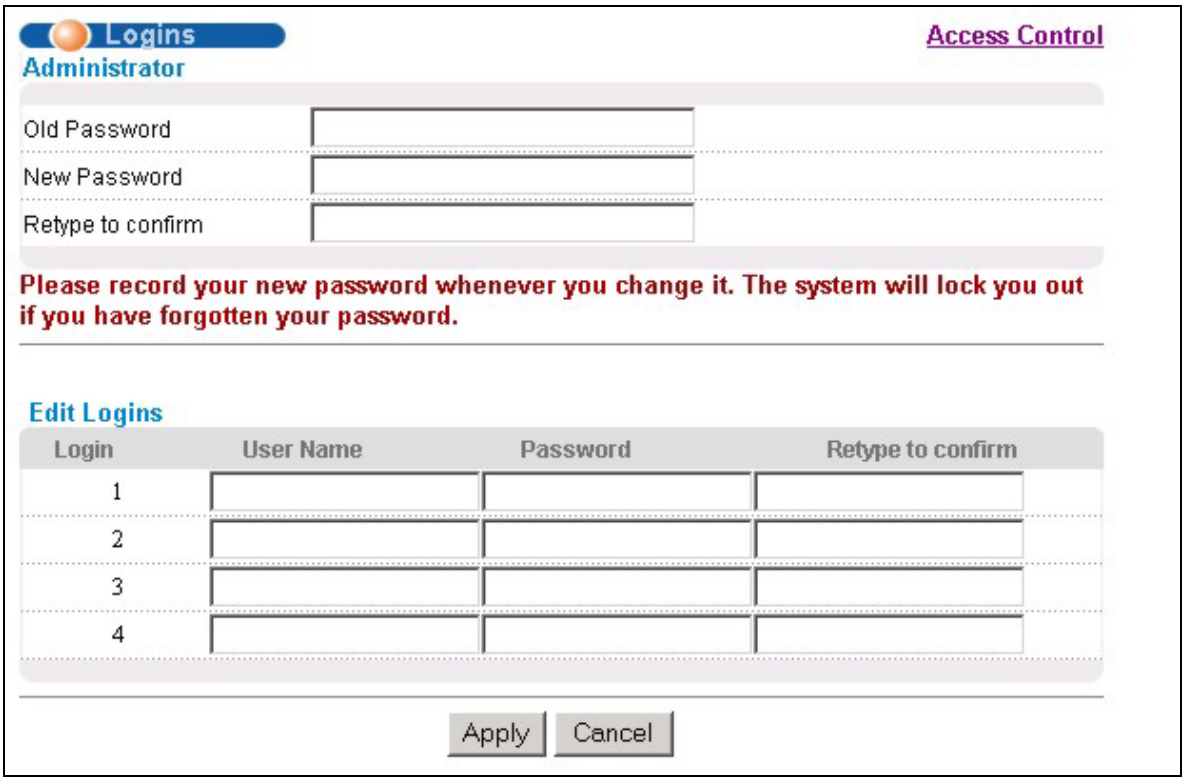


Figure 15-5 Access Control: Logins

The following table describes the labels in this screen.

Table 15-5 Access Control: Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the "admin" user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password ("1234" is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These people have read-only access.	
User Name	Set a user name (up to 30 characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes back to the switch.

Table 15-5 Access Control: Logins

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.4 Service Access Control

Service Access Control allows you to decide what services you may use to access the VES. You may also change the default service port and configure "trusted computer(s)" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the **Access Control** screen.

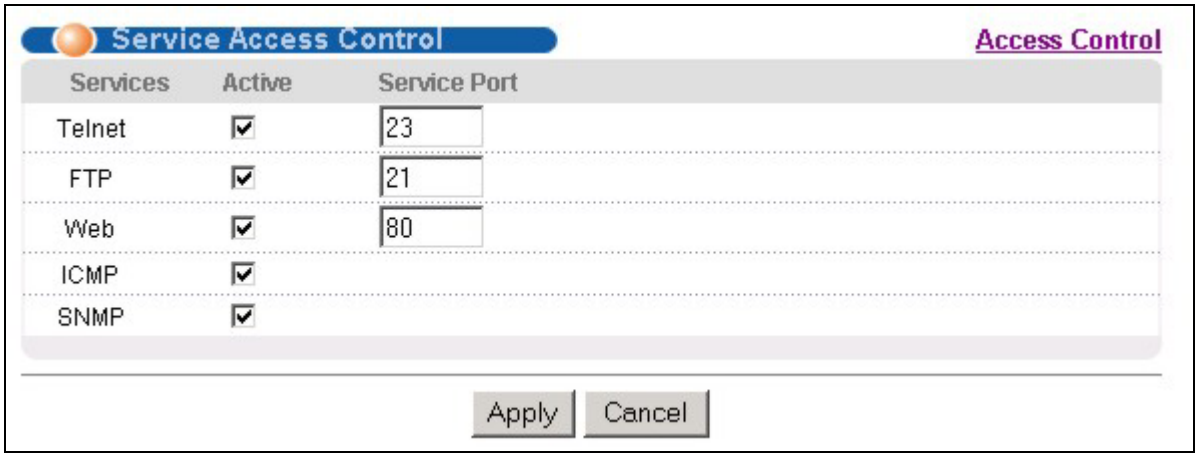


Figure 15-6 Access Control: Service Access Control

The following table describes the fields in this screen.

Table 15-6 Access Control: Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the switch are listed here.
Active	Select the **Active** check boxes for the corresponding services that you want to allow to access the switch.
Service Port	For Telnet, FTP or web services, you may change the default service port by typing the new port number in the **Service Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.5 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the VES. Click **Access Control** to return to the **Access Control** screen.

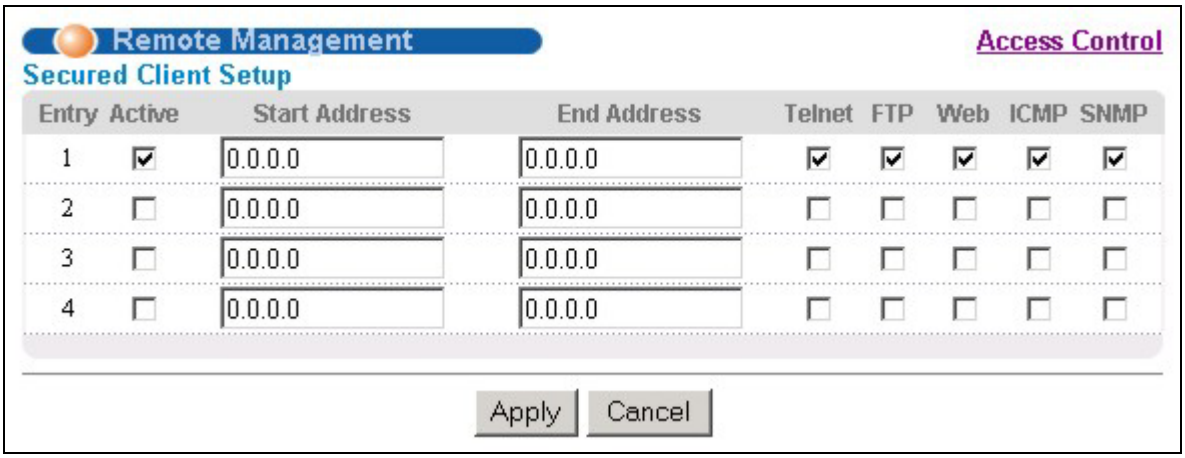


Figure 15-7 Access Control: Remote Management

The following table describes the labels in this screen.

Table 15-7 Access Control: Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers fro which you can manage this switch. The switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The switch immediately disconnects the session if it does not match.
Telnet/FTP/Web/ ICMP/SNMP	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 16 Queuing Method

This chapter introduces the switch's queuing algorithms.

16.1 Introduction to Queuing

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **Priority** in **Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

VES has two physical queues, high and low.

16.1.1 First Come First Serve

First come first serve queuing treats all traffic with the same priority. The switch transmits the traffic in the order it receives it. The high-priority queue does not get any priority over the low-priority queue.

16.1.2 Strict Priority Queuing

Strict priority queuing services queues based on priority only. As traffic comes into the switch, traffic in the high-priority queue is transmitted first. When the high-priority queue empties, traffic in the low-priority queue, is transmitted until the low-priority queue empties. If the high-priority queue never empties, then traffic in the low-priority queue never gets sent. Strict priority queuing does not automatically adapt to changing network requirements.

16.1.3 Weighted Round Robin Scheduling

Weighted round robin scheduling services queues based on the ratio determined by their queue weights (the numbers you configure in the **High Weight** or **Low Weight** field – see *Figure 16-1*). A queue with a larger weight gets more service than a queue with a smaller weight. This queuing mechanism is highly efficient in that it divides the available bandwidth across the different traffic queues. If one queue is empty, the switch just sends from the other queue. See *section 16.3* for an example of weighted round robin scheduling.

16.2 Configuring Queuing

Click **Queuing Method** under **Advanced Application** in the navigation panel.

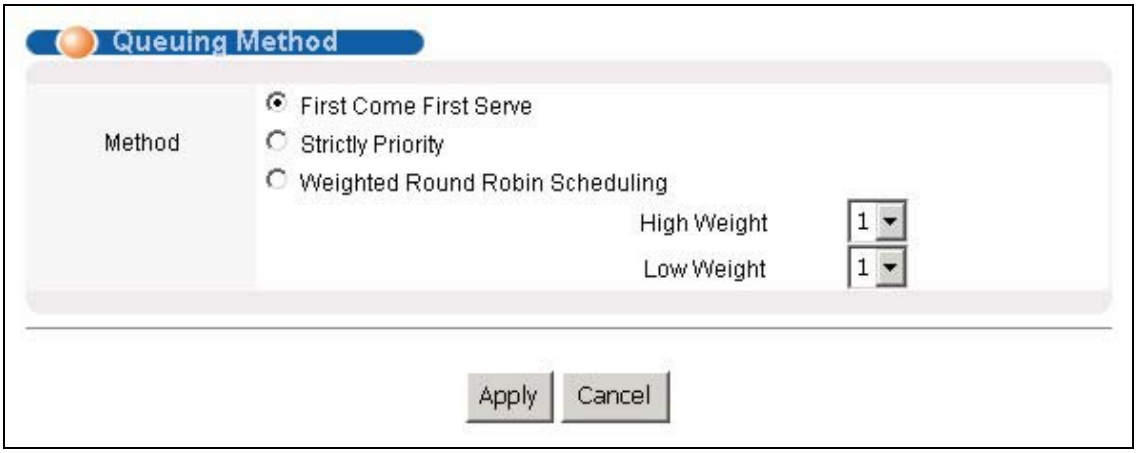


Figure 16-1 Queuing Method

The following table describes the labels in this screen.

Table 16-1 Queuing Method

LABEL	DESCRIPTION
Method	Select **First Come First Serve**, **Strictly Priority** or **Weighted Round Robin Scheduling**. First come first serve queuing treats all traffic with the same priority. The switch transmits the traffic in the order it receives it. The high-priority queue does not get any priority over the low-priority queue. Strictly priority queuing services queues based on priority only. When the high-priority queue empties, traffic on the low-priority queue begins. Weighted round robin scheduling services queues based on the ratio determined by their queue weights that you configure in the **High Weight** and **Low Weight** fields. Bandwidth is divided between the high and low traffic queues according to their weights. A queue with a larger weight gets more service than a queue with a smaller weight.
High Weight	Configure this field when you select **Weighted Round Robin Scheduling** in the **Method** field. Select a weight (1-7) for the high-priority queue traffic. This sets the ratio of how much high-priority queue traffic the switch transmits in relation to the amount of low-priority queue traffic (see the **Low Weight** field).
Low Weight	Configure this field when you select **Weighted Round Robin Scheduling** in the **Method** field. Select a weight (1-7) for the low-priority queue traffic. This sets the ratio of how much low-priority queue traffic the switch transmits in relation to the amount of high-priority queue traffic (see the **High Weight** field).
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.3 Weighted Round Robin Scheduling Example

This is an example of using **Weighted Round Robin Scheduling** as the queuing method. In this example the high-priority traffic's weight is set to **5** and the low-priority traffic's weight is set to **3**.

Figure 16-2 Weighted Round Robin Scheduling Configuration Example

With this configuration, the VES sends five frames from the high-priority queue for every three frames it sends from the low-priority queue (on average). In other words, as long as both queues are full, on average five eighths of the frames the switch sends are from the high-priority queue and three eighths are from the low-priority queue.

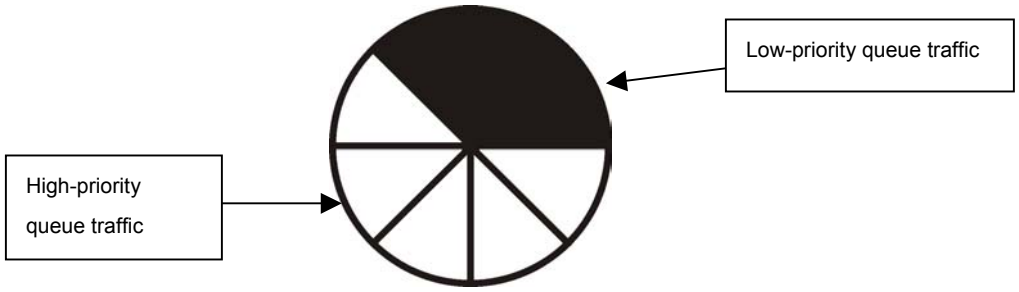


Figure 16-3 Weighted Round Robin Scheduling Ratio Example

Part V:

Routing Protocol and Management

This part describes the Routing Protocol and Management screens.

Chapter 17 Routing Protocol

This chapter shows you how to configure the static routing function.

17.1 Static Route

Static routes tell the VES how to forward the VES's own IP traffic when you configure the TCP/IP parameters manually. This is generally useful for allowing management of the switch from a device with an IP address on a different subnet from that of the switch's IP address (remote management).

Click **Routing Protocol** in the navigation panel and then **Static Routing** to display the screen as shown.

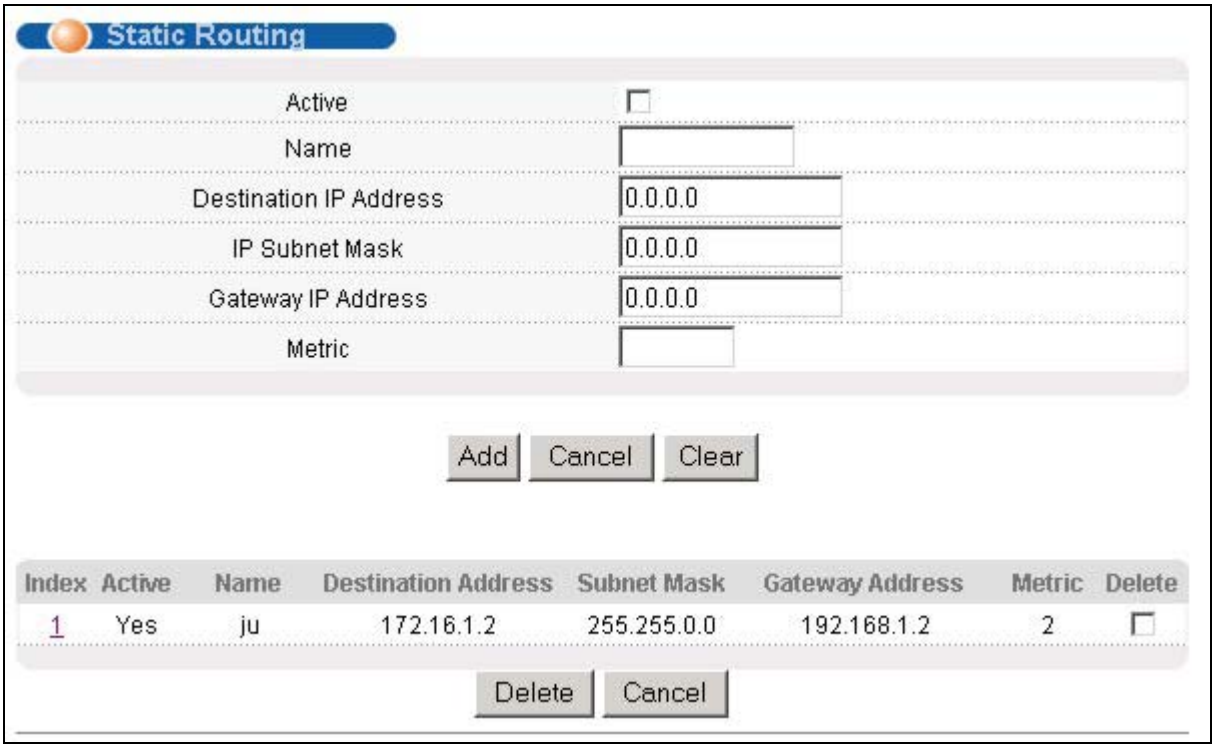


Figure 17-1 Static Routing

The following table describes the related labels you use to create a static route.

Table 17-1 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name for this route. This is for identification purpose only.

Table 17-1 Static Routing

LABEL	DESCRIPTION
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.

View the current static routes on the switch in the summary table at the bottom of the screen.

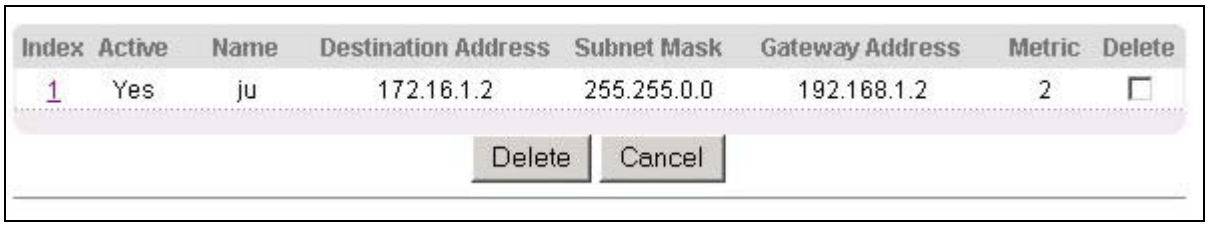


Figure 17-2 Static Routing: Summary Table

The following table describes the labels in the summary table.

Table 17-2 Static Routing: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.

Table 17-2 Static Routing: Summary Table

LABEL	DESCRIPTION
Metric	This field displays the cost of transmission for routing purposes.
Delete	Check the rule(s) that you want to remove in the **Delete** column, and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkboxes in the **Delete** column.

Chapter 18 Maintenance

This chapter explains how to configure the maintenance screens. The links on the upper right of the Maintenance screen lead to different screens that let you maintain the firmware and configuration files.

18.1 Maintenance

Click **Management** and then **Maintenance** in the navigation panel to open the following screen.

Figure 18-1 Maintenance

18.2 Firmware Upgrade

1. Click **Firmware Upgrade** in the **Maintenance** screen if you want to upgrade your switch firmware. See the **System Info** screen to verify your current firmware version number. Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

   ☞ **Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.**

2. From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

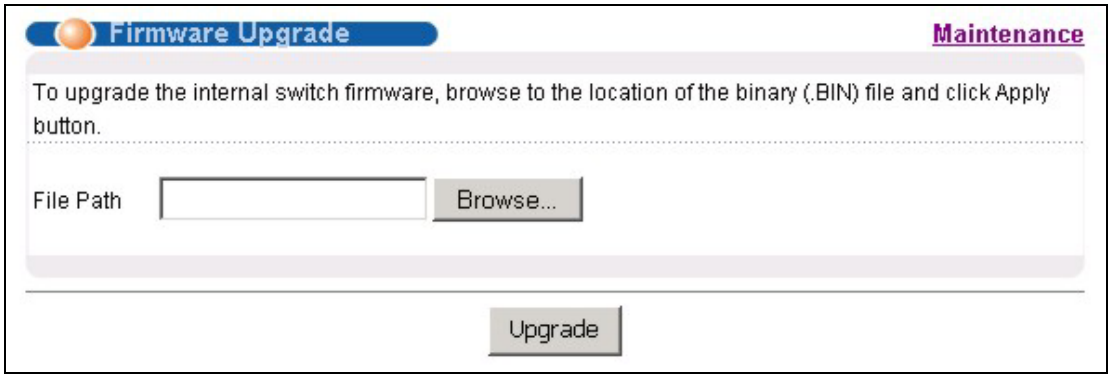

Firmware Upgrade
Maintenance
To upgrade the internal switch firmware, browse to the location of the binary (.BIN) file and click Apply button.
File Path
Browse...
Upgrade

Figure 18-2 Firmware Upgrade

3. Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

18.3 Restore a Configuration File

Restore a previously saved configuration from your computer to the switch using the **Restore Configuration** screen.

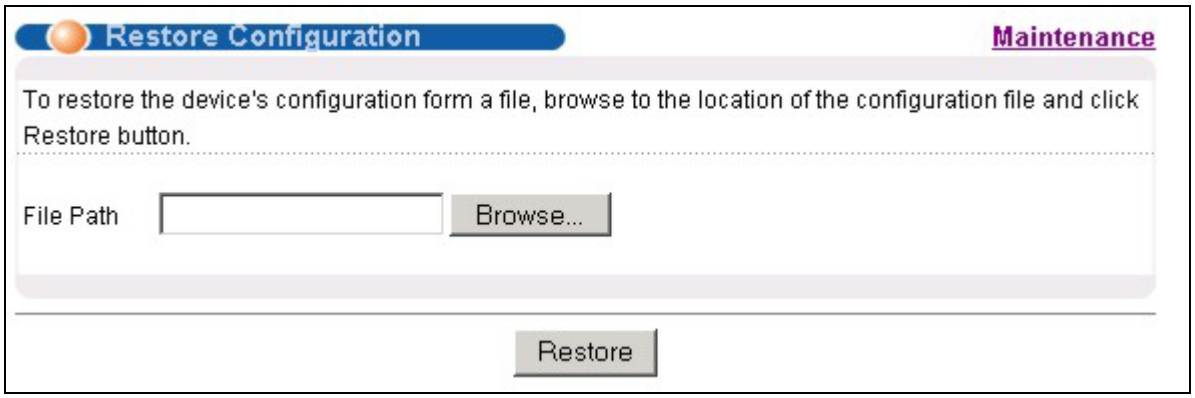

Restore Configuration
Maintenance
To restore the device's configuration form a file, browse to the location of the configuration file and click Restore button.
File Path
Browse...
Restore

Figure 18-3 Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display a **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "rom-0" is the name of the configuration file on the switch, so your backup configuration file is automatically renamed when you restore using this screen.

18.4 Backing Up a Configuration File

Backing up your switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current switch configuration to a computer using the **Configuration Backup** screen.

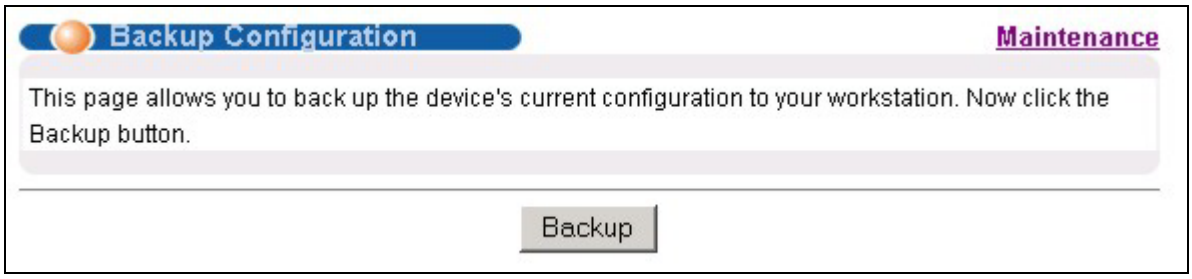

Backup Configuration
Maintenance
This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.
Backup

Figure 18-4 Backup Configuration

Follow the steps below to back up the current switch configuration to your computer in this screen.

1. Click **Backup**.
2. Click **Save** to display the **Save As** screen.
3. Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

18.5Load Factory Defaults

1. Press the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 18-5 Confirm Load factory Defaults

2. Click **OK** to go to the next screen.

Figure 18-6 Restart Switch After Load Factory Defaults

3. Click **OK** to begin resetting all switch configurations to the factory defaults and then wait for the switch to restart. This takes up to two minutes. If you want to access the switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default switch IP address (192.168.1.1).

18.6 Reboot System

Reboot System allows you to restart the switch without physically turning the power off. Press the **Click Here** button next to **Reboot System** to display the next screen.

Figure 18-7 Confirm Restart the Switch

Click **OK** in the screen that asks if you are sure you want to reboot the system. You then see the screen as shown in *Figure 18-6*. Click **OK** again and then wait for the switch to restart. This takes up to two minutes. This does not affect the switch's configuration.

18.7 Command Line FTP

This section shows some examples of uploading to or downloading files from the switch using FTP commands. First, understand the filename conventions.

18.7.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the screens such as password, switch setup, IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 18-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	This is the configuration filename on the switch. Uploading the rom-0 file replaces the entire ROM file system, including your switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the switch .

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the switch only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

18.7.2 FTP Command Line Procedure

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your switch.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "bin" to set transfer mode to binary.
6. Use "`put`" to transfer files from the computer to the switch, for example, "`put firmware.bin ras`" transfers the firmware on your computer (firmware.bin) to the switch and renames it "ras". Similarly, "`put config.rom rom-0`" transfers the configuration file on your computer (config.rom) to the switch and renames it "rom-0". Likewise "`get rom-0 config.rom`" transfers the configuration file on the switch to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.
7. Enter "`quit`" to exit the ftp prompt.

18.7.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 18-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.

Table 18-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

18.7.4 FTP over WAN Restrictions

FTP over WAN will not work when:

- Telnet service is disabled in **Secured Client Sets**.
- The IP address(es) in the **Secured Client Sets** menu does not match the client IP address. If it does not match, the switch will disconnect the Telnet session immediately.

Chapter 19 Diagnostic

This chapter explains the Diagnostic screens.

19.1 Diagnostic

Click **Management** and then **Diagnostic** in the navigation panel to display this screen. Use this screen to check system logs, ping IP addresses or perform loopback test on a port.

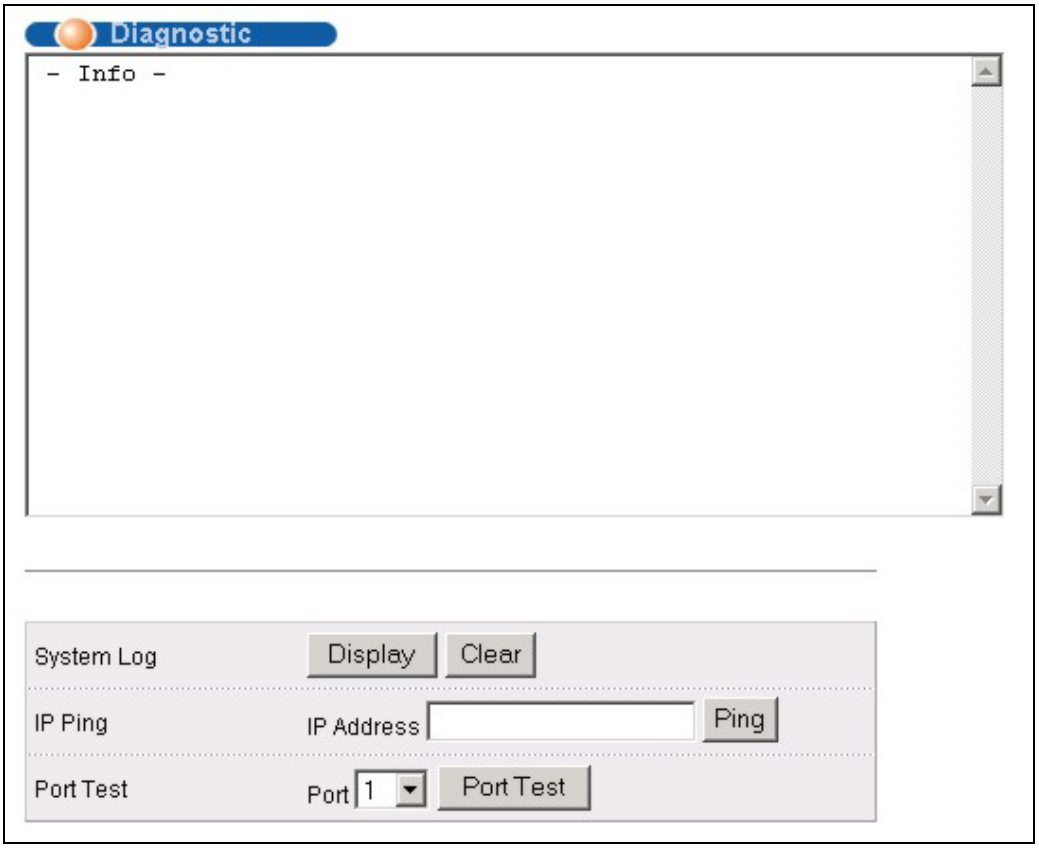


Figure 19-1 Diagnostic

The following table describes the labels in this screen.

Table 19-1 Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.

Table 19-1 Diagnostic

LABEL	DESCRIPTION
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the switch ping the IP address (in the field to the left) three times.
Port Test	From the **Port** drop-down list box, select a port number and click **Port Test** to perform VDSL loopback test.

Chapter 20
Cluster Management

This chapter introduces cluster management.

20.1 Introduction to Cluster Management

Cluster management1 allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 20-1 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch A in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

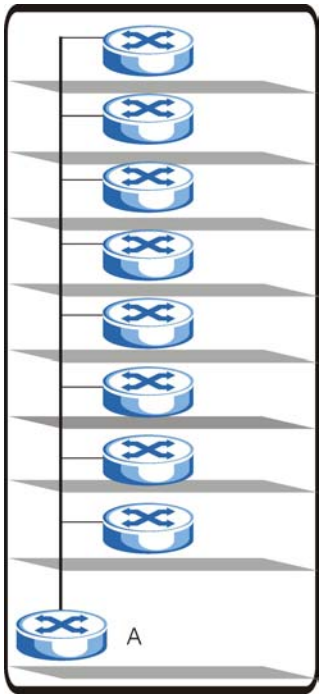


Figure 20-1 Clustering Application Example

1 Cluster management may also be referred to as "iStacking" in other ZyXEL documentation.

20.2 Cluster Management Status

Click **Management** in the navigation panel and then **Cluster Management** to display the following screen.

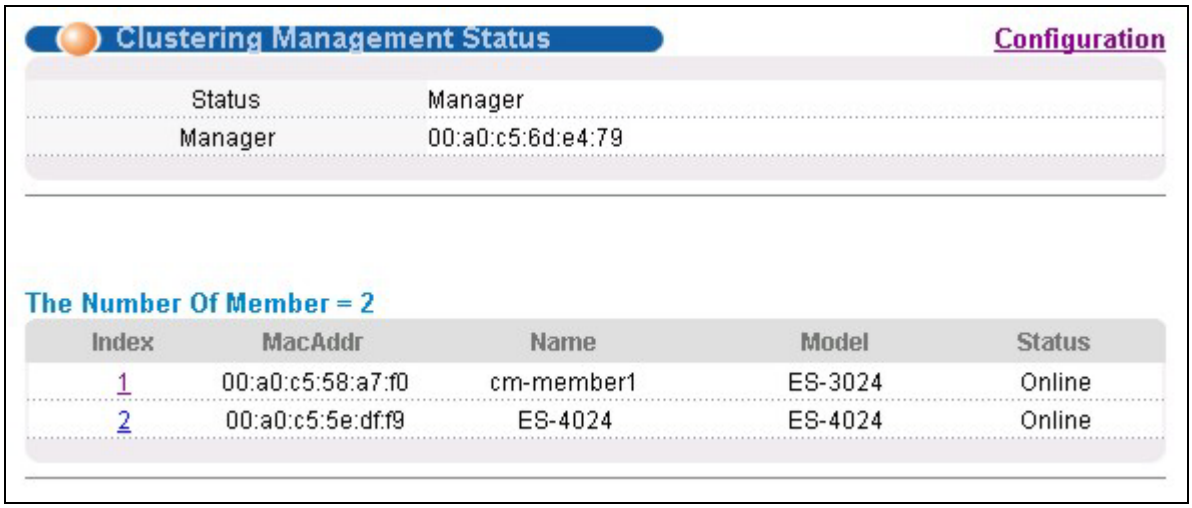


Figure 20-2 Cluster Management Status

The following table describes the labels in this screen.

Table 20-2 Cluster Management Status

LABEL	DESCRIPTION
A cluster can only have one manager.	
Status	This field displays the role of this switch within the cluster. o **Manager** o **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) o **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC Address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see *Figure 20-3*).
MacAddr	This is the cluster member switch's hardware MAC Address.
Name	This is the cluster member switch's **System Name**.
Model	This field displays the model name.

Table 20-2 Cluster Management Status

LABEL	DESCRIPTION
Status	This field displays: o **Online** (the cluster member switch is accessible) o **Error** (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) o **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down).

20.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different (see *Figure 20-3*).

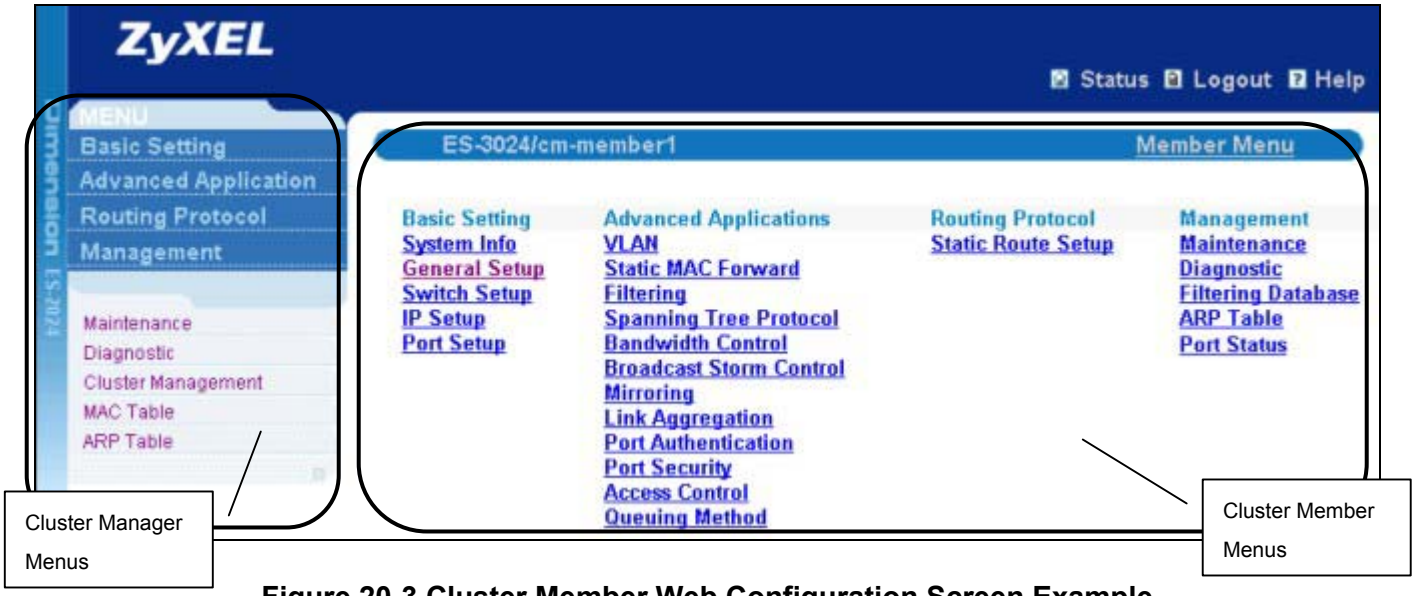


Figure 20-3 Cluster Member Web Configuration Screen Example

Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

```
C:\> ftp <Cluster Manager IP address>
User : <Enter>
Password: 1234 is the default password
230 Logged in
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         1399654 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          262144 Jul 01 12:00 rom-0
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-05-02-34
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-05-02-34
226 File sent OK
ftp: 462 bytes received in 0.01Seconds 30.80Kbytes/sec.
ftp> put 350DT3b1.bin fw-00-a0-c5-05-02-34
ftp> bye
```

Figure 20-4 Example: Uploading Firmware to a Cluster Member Switch

The following table explains some of the FTP parameters.

Table 20-3 FTP Upload to Cluster member Example

FTP PARAMETER	DESCRIPTION
User name	Press <Enter>
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
350DT3b1.bin	The name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-05-02-34	The cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-05-02-34	The cluster member switch's configuration file name as seen in the cluster manager switch.

20.3 Configuring Cluster Management

Click **Configuration** from the **Cluster Management** screen to display the next screen.

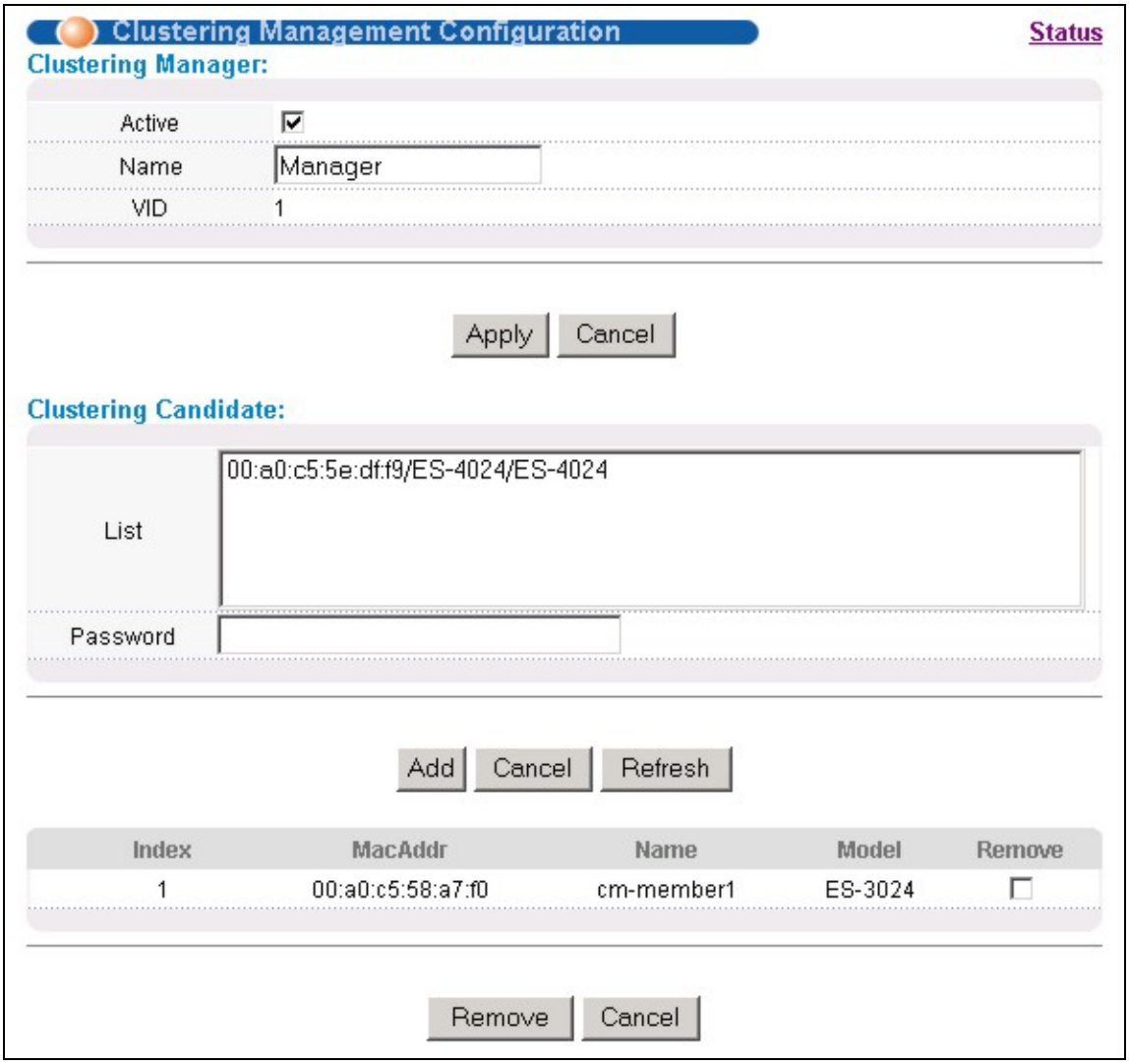


Figure 20-5 Configuring Cluster Management

The following table describes the labels in this screen.

Table 20-4 Configuring Cluster Management

LABEL	DESCRIPTION
Active	Select **Active** to have this switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon ( ) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 32 printable characters (no spaces are allowed).

Table 20-4 Configuring Cluster Management

LABEL	DESCRIPTION
VID	This is the Management VLAN ID and is only applicable if the switch is set to **802.1Q** VLAN. All switches must be in the same management VLAN group to belong to the same cluster. Switches that are not in the same management VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** to save these changes to the switch.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon ( ) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Apply	Click **Apply** to save these changes to the switch.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the devices selected for clustering.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.

Chapter 21 MAC Table

This chapter introduces the MAC Table.

21.1 Introduction to MAC Table

The MAC table shows how frames are forwarded or filtered across the switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the switch) or static (manually entered in **Static MAC Forwarding**).

The switch uses the MAC table to determine how to forward frames. See the following figure.

1. The switch examines a received frame and learns the port on which this source MAC address came.
2. The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.
   - If the switch has already learned the port for this MAC address, then it forwards the frame to that port.
   - If the switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
   - If the switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

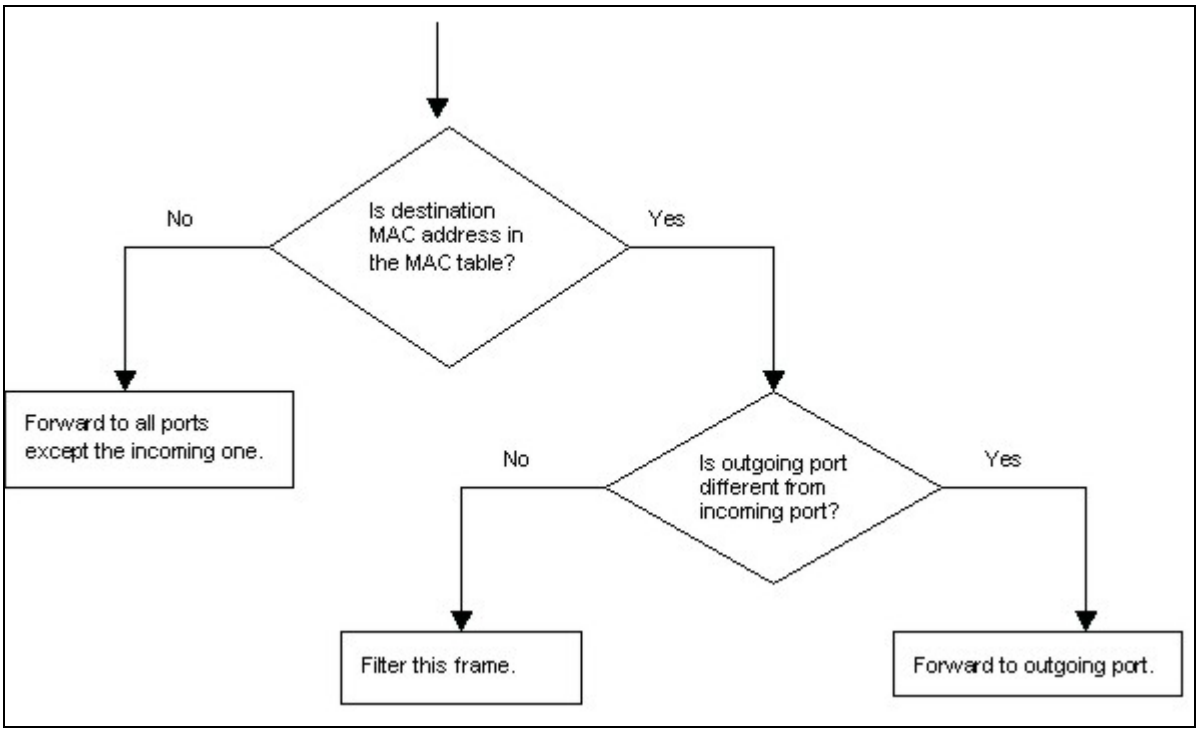


Figure 21-1 MAC Table Filtering Flowchart

21.2Viewing MAC Table

Click **Management** in the navigation panel and then **MAC Table** to display the following screen. The MAC table can hold up to [illegible] entries.

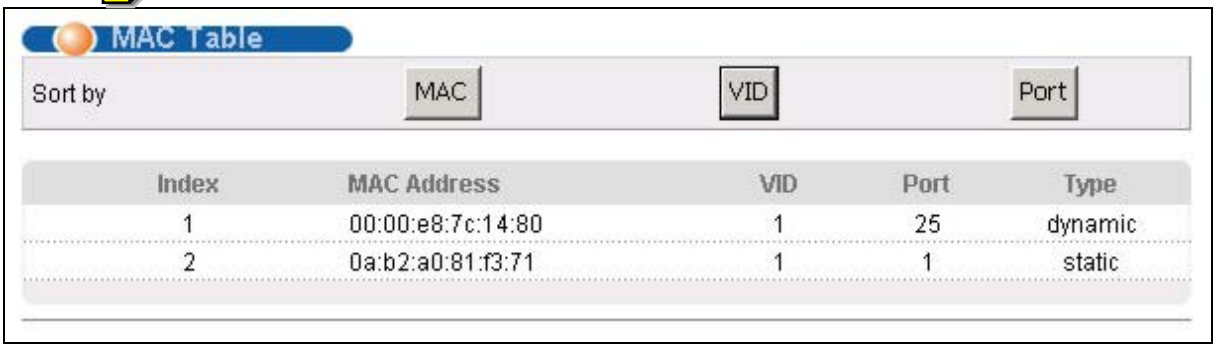


Figure 21-2 MAC Table

The following table describes the labels in this screen.

Table 21-1 MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in **Static MAC Forwarding**).

Chapter 22 ARP Table

This chapter introduces ARP Table.

22.1 Introduction to ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

22.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

22.2 Viewing ARP Table

Click **Management** in the navigation panel and then **ARP Table** to open the following screen. The ARP table can hold up to 500 entries.

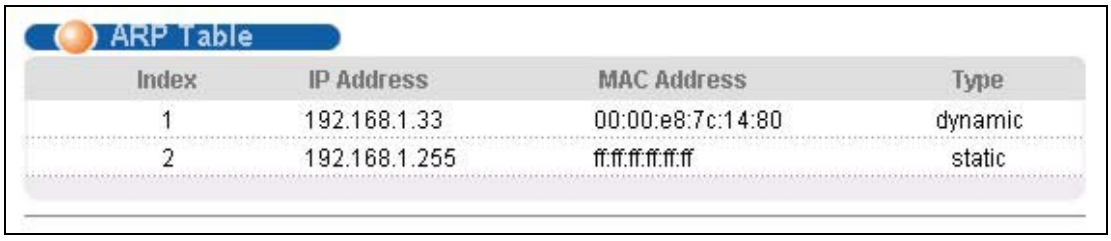


Figure 22-1 ARP Table

The following table describes the labels in this screen.

Table 22-1 ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in **Static MAC Forwarding**).

Part VI:

Commands

This part gives information on Command Line Interface (CLI) commands for the VES-1124.

Chapter 23 Introduction to CLI

This chapter introduces line commands and gives a summary of commands available.

23.1 Command Line Interface Overview

In addition to the web configurator, you can use line commands to configure the switch. It is recommended that you use the web configurator for everyday management of the switch and that you use line commands for advanced switch diagnosis and troubleshooting. If you have problems with your switch, customer support may request that you issue some of these commands to assist them in troubleshooting.

You can use the "config save" command to save 802.1Q, STP, Cluster and IP configuration changes to non-volatile memory (Flash). These changes are effective after you restart the switch.

However you cannot use "config save" for all other line command configurations. These are saved in volatile memory (DRAM), so are not effective after you restart the switch.

23.1.1 Accessing the Command Line Interface

There are two ways to access the command line interface on the VES:

- Telnet to the switch
- Connect a computer to the console port and use terminal emulation software configured to the following parameters:
  - VT100 terminal emulation
  - No parity, 8 data bits, 1 stop bit
  - 9600 bps
  - No flow control

23.1.2 Command Conventions

The system uses a one-level command structure. You must type the full command every time, as follows.

```
192.168.1.1> <command>
```

For instance, the following example shows how to enable GVRP.

```
192.168.1.1> sys sw gvrp enable
```

The conventions for typing in most CI commands are shown next.

```
command <interface|device> subcommand [parameter]
command subcommand [parameter]
```

Type all commands as displayed on the screen.

23.1.3 Command Syntax Conventions

- Command keywords are in `courier new` font.
- The `|` symbol means "or".
- Required fields in a command are enclosed in angle brackets <>. Use the following command to turn the system monitor on or off.

  ```
  sys monitor enable <on/off>
  ```

- Optional fields in a command are enclosed in square brackets `[]`, for example, year, month and day are optional in the following command. This command just displays the date if you don't specify the year, month and day parameters.

  ```
  sys date [year month day]
  ```

- Commands can be abbreviated to the smallest unique string that differentiates the command. For example the "system date" command could be abbreviated to "s d".

23.1.4 Getting Help

Type "`help`" or "`?`" to display a list of valid commands or type a command followed by "`help`" or "`?`" to display a list of associated subcommands.

The following figure shows a sample help information.

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
VES-1124> ?
Valid commands are:
sys             exit            device          ether
config          vdsl            bridge          monitor
ip              ppp             hdap
VES-1124>
```

Figure 23-1 CLI Help: Sample Output

23.2 Command Summary

The following tables are summaries of the commands available in the VES together with a brief description of each command. See the related section in the *User's Guide* for more background information.

23.2.1 sys Commands

Table 23-1 Command Summary: sys

COMMAND			DESCRIPTION
sys			

Table 23-1 Command Summary: sys

COMMAND			DESCRIPTION
	adjtime		Retrieves the date and time from the time server specified in the web configurator.
	cluster		
		active <name>	Assign a cluster name and enable clustering it.
		inactive <name>	Disable the cluster named.
		add <MAC addr> <password>	Add a member switch into the cluster using its web configurator password.
		remove <MAC addr>	Remove a member switch from the cluster.
		showMember	Shows details of member switches in this cluster.
		showCandidate	Shows a list of auto-discovered potential cluster members.
		status	Shows whether this switch is a cluster member, cluster manager or neither and information about members in the cluster.
		trace	Sets the cluster management debug level.
		active <name>	Assign a cluster name and enable clustering it.
	countrycode	<country code>	Sets or displays the firmware country code.
	cpu	display	Displays the CPU's utilization.
	date	[year month day]	Sets or displays the system's current date.
	domainname	[domain name]	Sets or displays the system domain name.
	edit		Edits the system preset text file such as autoexec.net.
	fanstatus		Displays the current operational state of the switch's fan.
	feature		Displays a list of the device's major features.
	hostname	[hostname]	Sets or displays the system name.
	log		
		clear	Clears the error log.
		disp	Shows the error log.

Table 23-1 Command Summary: sys

COMMAND			DESCRIPTION
		online [on|off]	Enables/disables the error log to be displayed on screen.
	romreset		Sets the switch back to the factory default settings.
	snmp	getCommunity <index> [<community>]	Sets or displays the SNMP GetRequest community.
		setCommunity <index> [<community>]	Sets or displays the SNMP SetRequest community.
		trustedHost <index>[<host>]	Sets or displays the SNMP trusted host.
		trapCommunity <index> [<community>]	Sets or displays the SNMP Trap community.
		trapDest <index>[<destination>]	Sets or displays the SNMP trap server.
		disp <index|all>	Shows SNMP settings.
	socket		Displays the system socket's ID #, type, control block address (PCB), IP address and port number of peer device connected to the socket (Remote Socket) and task control block (Owner).
	stdio	[minute]	Sets or displays the management terminal idle timeout value.
	syslog	server	Set syslog server IP address
		facility	Set syslog facility
		type	Set/display syslog type flag
		mode	Set syslog mode
	time	[hour [min [sec]]]	Sets or displays the system time.
	trcdisp	parse, brief, disp	Sets the level of detail that should be displayed. Use "parse" to display the most detail and "disp" to display the least.
	trclog		
		switch [on|off]	Enables/disables/ the system trace log or shows whether it's on or off.
		online [on|off]	Enables/disables the trace log onscreen display (for example in the telnet management window).
		level [level]	Sets the level (1-10) of trace logs (1 shows the least) to display.
		type <bitmap>	Uses hexadecimal characters to set the type of trace logs to record.

Table 23-1 Command Summary: sys

COMMAND			DESCRIPTION
		disp	Shows the trace log.
		clear	Erases the trace log.
		encapmask [mask]	Shows which type of encapsulation the trace log records or sets it if you specify the encapsulation's hexadecimal character.
	trcpacket		
		create <entry> <size>	Creates a packet trace buffer.
		destroy	Removes the packet trace buffer.
		channel <name> [none|incoming|outgoing|bothway]	Sets the packet trace direction for a given channel.
		string [on|off]	Enables/disables the sending of a log to the trace packet buffer when configuration changes are made or displays the current setting.
		switch [on|off]	Enables/disables packet trace or displays the current setting.
		disp	Displays the trace packets.
		udp	Sends the trace packets to another system using UDP.
		udp switch [on|off]	Enables/disables the sending of the trace packets to another system using UDP or displays the current setting.
		udp addr <addr>	Sets the target IP address for sending trace packets using UDP.
		udp port <port>	Sets the UDP port (should match that of the target IP address) for sending trace packets using UDP.
		parse [[start_idx], end_idx]	Displays detailed packet details of the packet range specified.
		brief	Displays a brief listing of packet contents.
	version		Displays the RAS code and driver versions.
	view	view <filename>	Displays the specified text file.
	wdog		
		switch [on|off]	Turns the watchdog firmware protection feature on or off.
		cnt [value]	Sets (0-34463) or displays the current watchdog count (in 1.6 sec units).

23.2.2 sys sw Commands

The following commands are system switch commands; all are preceded with `sys sw`

Table 23-2 Command Summary: sys sw

COMMAND			DESCRIPTION
driver	config		Shows the switch's settings.
	count	disp	Shows the switch Network Driver Interface Specifications (NDIS) level counters (CPU interface).
		clear	Clears the switch NDIS level counters (CPU interface).
garp	status		Shows the GARP timer status.
	timer	<join timer(ms)><leave timer(ms)><leave all timer<ms>	Sets the GARP timer's Join Timer, Leave Timer and Leave All Timer.
gvrp	trace		Sets GVRP trace level.
	status		Shows the GVRP status.
	enable		Enables GVRP.
	disable		Disables GVRP.
pktcnt	<port 1-26>		Display port statistic counter.
pktcntclear	<port 1-26>		Reset port statistic counter.
pktsend			
port	<portID> <enable | disable> <Speed> <FlowCtrl>		Port setup.
portstatus			Displays current port status and settings.
phyread	<portID> [<phyAddr>]		Reads PHY register.
phywrite	<portID> <phyAddr> <data>		Writes PHY register.
qos	defpri	<port> [<0:none | 1:low | 2:high>]	Sets the default ingress User Priority for a port.
	map	<0..7> [<0:low | 1:high>]	Maps a User Priority to a Traffic Class.
	method	<0:FCFS | 1:Strict | 2:WRR [high weight] [low weight]>	Sets the QoS method.
	showmethod		Displays the QoS method.
vlan1q			All "sys sw vlan1q" commands relate to IEEE 802.1Q Tagged VLAN configuration. Use "config save" to save your configuration changes.
	port	status <port>	Shows a port's VLAN information.

Table 23-2 Command Summary: sys sw

COMMAND			DESCRIPTION
		defaultVID <port><vid>	Sets the default VLAN ID of a port.
		accept <port> <all|tagged|untagged>	Sets the type of frames that a port accepts.
		gvrp <port> <enable|disable>	Enables/disables GVRP on the specified port.
	svlan	cpu <vlan id>	Sets the VLAN ID of the management VLAN (CPU).
		setentry<name><vid><port><adctl> <tagctl>	Applies a static VLAN (name, admin control tag, tag control) to a port.
		delentry <vid>	Deletes the specified (VID) static VLAN.
		active <vid>	Turns on the specified static VLAN.
		inactive <vid>	Turns off the specified static VLAN.
		list	Displays a table of static VLANs.
	vlan	list <all|vid|start_vid end_vid>	Shows the specified IEEE 802.1Q Tagged VLAN table.
	status		Shows the IEEE 802.1Q tagged status.
rstp			All "sys sw rstp" commands relate to rapid STP configuration. Refer to IEEE Std 802.1w. Use "config save" to save your configuration changes.
	bridge		
		enable	Enables RSTP.
		disable	Disables RSTP.
		priority <priority>	Sets the system priority.
		maxage <Max_Age>	Sets the max age timer
		hellotime <Hello_Time>	Sets the hello timer.
		forwardDelay <Forward_Delay_Time>	Sets the forward delay time
		version <STP:0|RSTP:2>	Displays/enables the STP mode; STP or RSTP. RSTP is the default used when configuring STP via web configurator.
	port		
		enable <port_no>	Enables RSTP on this port.
		disable <port_no>	Disables RSTP on this port.

Table 23-2 Command Summary: sys sw

COMMAND			DESCRIPTION
		pathCost <Port_NO> <Cost|0:Auto>	Sets the specified port's path cost.
		priority <Port_NO> <Priority>	Sets the specified port's priority.
		edgeport <port_no>	Displays if this port is an edge port.
		p2pLink <Port_NO> <Auto:2|True:1|False:0>	Sets whether the specified port can connect to one bridge or multiple bridges.
		mcheck <Port_NO>	Enables the Port Protocol Migration state machine (Disabled, Blocking, Listening, Learning, Forwarding) on the specified port.
	disp		Shows the RSTP runtime status.
	trace	[level]	Sets the RSTP debug level.
lacp			Refer to IEEE 802.3ad for more information on link aggregation control protocol (LACP. It is recommended that you use the web configurator to configure LACP parameters.
	agg		Displays aggregated ports.
	port		
		enable <port_no>	Enables LACP on the specified port.
		disable <port_no>	Disables LACP on the specified port.
		status <port_no>	Displays whether LACP is enabled on the specified port.
		actoradm activity [port_no] [0:passive 1:active]	Allows/disallows the specified local port to engage in link aggregation.
		actoradm display [port_no]	Shows whether the specified local port is engaged in link aggregation.
		actoradm key [port_no][key]	Shows the specified local port LACP key.
		actoradm priority [port_no] [priority]	Sets the specified local port LACP priority.
		actoradm timeout [port_no] [0:long_timeout|1:short_timeout]	Enables a short or long timeout on the specified local port.
	keymgnt	[on|off]	Turns LACP key management on or off.

Table 23-2 Command Summary: sys sw

COMMAND			DESCRIPTION
	syspriority	<priority>	Sets the LACP system priority. The switch with the lowest priority becomes the LACP "server".
	trace	[level]	Sets the LACP debug level.
dot1x			"sys sw dot1x" commands relate to IEEE 802.1X security.
	enable		Enables 802.1X security on the switch.
	disable		Disables 802.1X security on the switch.
	status		Shows switch 802.1X security status.
	port		
		enable <port_no>	Enables 802.1X security on the specified port.
		disable <port_no>	Disables 802.1X security on the specified port.
		reauth <port_no> <on|off>	Turns re-authentication on or off on the specified port.
		period <port_no><value>	Configures how often the specified port should be re-authenticated.
		status <port_no>	Displays 802.1X security status on the specified port.
	set		
		radius server <ip>	Sets the external RADIUS server IP address.
		radius secret <secret>	Sets the external RADIUS server password.
		radius port <port>	Sets the external RADIUS server port number.
		radius show	Displays the external RADIUS server settings.
bmstorm			These commands relate to broadcast storm control.
	enable		Turns on broadcast storm control.
	disable		Turns off broadcast storm control.
	disp		Displays broadcast storm control ports' settings.

Table 23-2 Command Summary: sys sw

COMMAND			DESCRIPTION
	set	<threshold: 1(5%) 2(10%) 3(15%) 4(20%) 5(25%)>	Specifies the threshold percentage of broadcast frames that triggers broadcast storm control.
mac	static		Displays static MAC addresses.
		display [<mac> <vid>]	Displays current run-time static MAC addresses on the ports.
		set <port> <MAC> <vid>	Configures a static MAC address on the specified port.
		del <port> <MAC> <vid>	Deletes a static MAC address on the specified port.
	ageSet	<timeout>	Sets aging timeout.
	ageView		Displays the aging timeout period.
	list	<all | port_no>	Displays the forwarding table entries.
	flush	[port]	Flushes learned MAC addresses in the forwarding table.
	count	[port]	Displays the number of MAC addresses in the forwarding table.
	search	<MAC> <VID>	Searches the MAC/VID learned on which port.
mirror			The following commands relate to port mirrors. Port mirroring is copying traffic from one or all ports to another or all ports for external analysis.
	enable		Turns on port mirroring.
	disable		Turns off port mirroring.
	display		Displays current run-time port mirror settings.
	set	<none | port_no...>	Sets the mirrored port (s) (the ports from which traffic is copied to another port for analysis).
	direction	<ingress | egress | both>	Sets the direction of mirrored traffic.
	port	<monitor port_no>	Sets the monitor port (the port to which traffic is copied for analysis).

Table 23-2 Command Summary: sys sw

COMMAND			DESCRIPTION
bw			The following commands relate to defining a maximum allowable bandwidth for incoming and/or outgoing traffic flows for specified ports.
	display	<port>	Displays current run-time bandwidth control settings.
	set	<port> <enable|disable> <ingress rate[kbps]> <egress rate[kbps]>	Enables or disables bandwidth control of ingress and/or egress rates on individual ports.
trunk			The following commands relate to trunking. Trunking is the grouping of physical ports into one logical higher-capacity link.
	del	<id>	Delete a trunk group.
	display		Displays current run-time trunk settings.
	listView		Displays member list of trunk.
	set	<id> <port_no...>	Sets members of a trunk group.
mc			
	set	<addr> <port>...	Sets ports to a specific multicast address.
	del	<addr>	Deletes a specific multicast address.
	get	<addr>	Shows a multicast address's forwarding ports.
vlan			
	status		Displays VLAN status
	type	<802.1q | port-based>	Sets VLAN mode

23.2.3 exit Command

Table 23-3 Command Summary: exit

COMMAND	DESCRIPTION
exit	Ends the console or telnet session.

23.2.4 ip Commands

Table 23-4 Command Summary: ip

COMMAND			DESCRIPTION
ip			
	address	[addr]	Displays the host IP address.
	alias	<iface>	Sets an alias for the specified interface.
	aliasdis	<0|1>	Disables/enables the alias for the specified interface.
	arp	status	Displays all interfaces' IP Address Resolution Protocol status.
	httpd	debug [on|off]	Enables or disables the HTTP debug flag.
	icmp		
		status	Displays the ICMP statistics counter.
		discovery <iface> [on|off]	Sets the ICMP router discovery flag.
	ifconfig	[iface] [ipaddr] [broadcast <addr> |mtu <value>|dynamic]	Configures a network interface.
	ping	<hostid>	Pings a remote host.
	route		
		status	Displays the routing table.
		add <dest addr>[/<bits>] <gateway> [<metric>]	Adds a route.
		addiface <dest addr>[/<bits>] <iface> [<metric>]	Adds an entry to the routing table for the specified interface.
		addprivate <dest addr>[/<bits>] <gateway> [<metric>]	Adds a private route.
		drop <host addr> [/<bits>]	Drops a route.
	status		Displays IP statistic counters.
	udp	status	Displays the UDP status.
	tcp		
		status [tcb] [<interval>]	Displays the TCP statistic counters.
	telnet	<host> [port]	Telnets to the specified host.
	traceroute	<host> [ttl] [wait] [queries]	Sends ICMP packets to trace the route of a remote host.
	igmpsnoop		
		status	Displays the IGMP group table.
		querier	Displays the port number of the incoming port that received the latest IGMP querier.

Table 23-4 Command Summary: ip

COMMAND			DESCRIPTION
		enable	Turns on IGMP snooping.
		disable	Turns off IGMP snooping.
	dhcp <iface>	mode <none | client>	Set an interface to accept information from a DHCP server.
	dhcp <iface>	status	Show whether an interface can accept information from a DHCP server.
	dhcp <iface>	client release	Release DHCP information such as the IP address from an interface
	dhcp <iface>	client renew	Renew the IP address on the interface.
	dns		
		stats clear	Clears DNS statistics.
		stats disp	Displays DNS statistics.

23.2.5 vdsl Command

Table 23-5 Command Summary: vdsl

COMMAND			DESCRIPTION
vdsl			
	active	[* | <chan_s> [<chan_e>]] [on | off]	This command actives/deactivates the VDSL channel(s).
	clear	[* |<chan_s> [<chan_e>]]	Clears VDSL related counters.
	condition	[* | <chan_s> [<chan_e>]]	Displays VDSL channels details.
	debug	[* | <chan_s> [<chan_e>]] [on | off]	This command sets the VDSL debug flag.
	enet		
		status [* | <chan_s> [<chan_e>]]	This command shows the VDSL status counters.
		clear [* | <chan_s> [<chan_e>]]	Clear VDSL related counters
		mdi [* | <chan_s> [<chan_e>]] <mode>	Sets the specified subscriber's modem's Ethernet port to either 0: auto, 1: MDI or 2: MDIX.
		monitor [* | <chan_s> [<chan_e>]] [on | off]	This command sets the VDSL monitor flag.
		phy [* | <chan_s> [<chan_e>]] [lt | nt]	Shows the Ethernet channel's PHY registers.

Table 23-5 Command Summary: vdsl

COMMAND			DESCRIPTION
		speed [* | <chan_s> [<chan_e>]] <speed>	Sets the speed of the channel.
		fctrl [* | <chan_s> [<chan_e>]] [on | off]	Turns the flow control on or off.
	monitor	<chan> [on | off]	This command sets the VDSL monitor flag.
	pbo	[* | <chan_s> [<chan_e>]] <pbo_id>	Sets power back off on the specified VDSL channel(s). 0: Table PBO 1: Chip Default PBO 2: Disable PBO
	pbooffset	[* | <chan_s> [<chan_e>]] <offset>	Adds offset to power back off.
	portdetail	[* | <chan_s>] [<chan_e>]	Shows the VDSL port details.
	power	[* | <chan_s> [<chan_e>]] [lt | nt] <value>	Sets the transmission power.
	profile		
		apply <profile_name> [*|vdsl01…vdsl24]	Activates a profile.
		delete <profile_name>	Removes a profile.
		get <profile_name>	Displays a profile's settings.
		list	Displays the settings of all the profiles.
		set <profile_name> <mode> <UpLnRate> <DownLnRate> <UpData> <DownData> [auto]	Sets profile parameters.
		reference	Displays a table showing the VDSL channels and their corresponding profiles.
	quality	[* | <chan_s> [<chan_e>]]	Shows VDSL upstream and down stream statistics.
	reset	[* | <chan_s> [<chan_e>]]	Resets a VDSL port.
	reconnect	[* | <chan_s> [<chan_e>]]	Reconnects a VDSL port.
	remotetest	[* | <chan>] <times>	Sends a VDSL remote loopback test packet to the subscriber's modem's VDSL chip.
	show	[* | <chan_s> [<chan_e>]]	This command shows VDSL settings.
	status	[* | <chan_s> [<chan_e>]]	This command shows the VDSL status counters.
	ver		This command shows the VDSL chip's modem code version.

23.2.6 config Command

Table 23-6 Command Summary: config

COMMAND		DESCRIPTION
config	save	You can use the "config save" command to save 802.1Q, STP, Cluster and IP configuration changes to non-volatile memory (Flash). These changes are effective after you restart the switch. However you cannot use "config save" for all other line command configurations. These are saved in volatile memory (DRAM), so are not effective after you restart the switch.

Chapter 24 Command Examples

This chapter describes some commands in more detail.

24.1 Commonly Used Commands Overview

These are commands that you may use frequently in configuring and maintaining your switch. See the following chapter for IEEE 802.1Q Tagged VLAN commands.

24.2 sys Commands

These are the commonly used commands that belong to the sys (system) group of commands.

24.2.1 sys log disp

Syntax:

```
sys log disp
```

This command displays the system error log. An example is shown next.

```
VES-1124> sys log disp
  38 Sat Jan  1 00:00:03 2000 PP02 -WARN  SNMP TRAP 3: link up
  39 Sat Jan  1 00:00:10 2000 PINI -WARN  SNMP TRAP 0: cold start
  40 Sat Jan  1 00:00:10 2000 PINI  INFO  main: init completed
  41 Sat Jan  1 00:00:15 2000 PP2b  INFO  adjtime task pause 1 day
  42 Sat Jan  1 00:10:16 2000 PP1b -WARN  SNMP TRAP 3: link up
  43 Sat Jan  1 00:10:16 2000 PP1b  INFO  Uplink25 Link Up
  46 Sat Jan  1 01:17:36 2000 PP1b -WARN  SNMP TRAP 2: link down
Clear Error Log (y/n):
```

Figure 24-1 sys log disp Command Example

24.2.2 sys log clear

Syntax:

```
sys log clear
```

This command clears the system error log.

If you clear a log (using the `sys log clear` command), you cannot view it again.

24.2.3 sys version

Syntax:

```
sys version
```

This command shows the RAS code, firmware version, system uptime and bootbase version.

An example is shown next.

```
VES-1124> sys version
 ZyNOS version: V3.50(LP.0)b1 | 05/05/2004
 romRasSize: 1220476
 system up time: 6:45:23 (2432246 ticks)
 bootbase version: V1.00(VES-1124) | 04/26/2004
 ZyNOS CODE: RAS VES1124 May 05 2004 16:55:28

 MAC Address: 00:a0:c5:01:23:45
VES-1124>
```

Figure 24-2 sys version Command Example

24.2.4 sys sw vlan1q vlan list

Syntax:

```
sys sw vlan1q vlan list <all | vid | start_vid end_vid>
```

where

`<all | vid | start_vid end_vid>=`	Specify either all of the VLAN entries (all), a single VLAN ID (vid) or a range of VLAN IDs starting from a certain VID (start_vid) or a range of VLAN Ids ending at a specific VID (`end_vid`).

This command displays the IEEE 802.1Q tagged VLAN table. An example is shown next.

```
VES-1124> sys sw vlan1q vlan list all
   No.   VID  ElapsedTime  Status  EgressPort/UntaggedPort
  ------ ---- -----------  ------  --------------------------------
    1)     1      0:05:43  Static  EEEEE|EEEEE|EEEEE|EEEEE|EEEEE|E
                                   UUUUU|UUUUU|UUUUU|UUUUU|UUUUU|U
VES-1124>
```

Figure 24-3 sys sw vlan1q vlan list Command Example

24.2.5 sys sw pktcnt

Syntax:

```
sys sw pktcnt <port>
```

This command displays statistics of a port. An example is shown next.

```
VES-1124> sys sw pktcnt 25
RxPkt64 = 4620
RxPkt65to127 = 2209
RxPkt128to255 = 1699
RxPkt256to511 = 595
RxPkt512to1023 =  414
RxPkt1024toMax =   13
RxOverSizePkt =    0
RxUnderSizePkt =    0
RxFCSErr =    0
RxAlignErr = 0
RxJabber =    0
RxFragment =    0
TxUcastPkt = 17448
TxNUcastPkt =  151
TxUnderrun =    0
TxExcesCollisn =    0
TxCollisn =    0
DropFwdLkup = 1395
DropInOverrun =    0
DropOutQueLife =    0
VES-1124>
```

Figure 24-4 sys sw pktcnt Command Example

24.2.6 sys sw mac list

Syntax:

```
sys sw mac list <all | port_no>
```

This command displays the MAC address(es) stored in the switch. An example is shown next.

```
VES-1124> sys sw mac list all

 ADDR       MACADDR      FID  STA  IsTrkGrp  Port#  HiPriDmac HiPriSmac

======  ==============  ====  ===  ========  =====  ========= =========
  9154    0005baad4f80  0002   01         00     26          00  00

======  ==============  ====  ===  ========  =====  ========= =========

Number of Static MACs: 1
Number of Dynamic MACs: 0
VES-1124>
```

Figure 24-5 sys sw mac list Command Example

24.3sys cluster Commands

These are the commonly used commands that belong to the "sys cluster" group of commands. Use "config save" to save these configurations.

24.3.1 sys cluster status

Syntax:

```
sys cluster status
```

This command shows whether this switch is a cluster member, cluster manager or neither and information about members in the cluster. An example is shown next.

```
VES-1124> sys cluster status
Cluster Info.
  Status: 1 (0:none, 1:manager, 2:slave)
  Name: 1
  number of members: 1,                member_p=411e20
  number of discover devices: 0,       list_p=4139e0
VES-1124>
```

Figure 24-6 sys cluster status Command Example

24.3.2 sys cluster showMember

Syntax:

```
sys cluster showMember
```

This command shows details of member switches in this cluster. An example is shown next.

```
test_mem> sys cluster showMember
No1
  ipAddr = 127.0.0.1
  mask = 255.255.0.0
  hwAddr = 00:a0:c5:05:02:34
  hostName = test_mem
  modelName=
  time = 100
  status = 4(0:Invalid, 1:waiting, 2:Active, 3:Inactive, 4:static)

No2
  ipAddr = 127.0.0.2
  mask = 255.255.0.0
  hwAddr = 00:a0:c5:05:22:11
  hostName = cm-member1
  modelName= VES-1124
  channel = swp05
  time = 90
  status = 2(0:Invalid, 1:waiting, 2:Active, 3:Inactive, 4:static)

No3
  ipAddr = 127.0.0.3
  mask = 255.255.0.0
  hwAddr = 00:a0:c5:3f:91:54
  hostName = VES-1124
  modelName= VES-1124
  channel = swp11
  time = 0
  status = 1(0:Invalid, 1:waiting, 2:Active, 3:Inactive, 4:static)
```

Figure 24-7 sys cluster showMember Command Example

24.3.3 sys cluster showCandidate

Syntax:

```
sys cluster showCandidate
```

This command shows a list of auto-discovered potential cluster members. An example is shown next.

```
test_mem> sys cluster showCandidate
NO.1
  hwAddr = 00:a0:c5:e8:e5:e3
  hostName=
  modelName=VLC-1000
  channel =
NO.2
  hwAddr = 00:a0:c5:77:77:77
  hostName=
  modelName=VLC-1000
  channel =
test_mem>
```

Figure 24-8 sys cluster status Command Example

24.4 ip Commands

These are the commonly used commands that belong to the ip group of commands. Use "config save" to save these configurations.

24.4.1 ip ping

Syntax:

```
ip ping <hostid>
```

This command pings a remote host. An example is shown next.

```
VES-1124> ip ping  192.168.1.16
Resolving 192.168.1.16... 192.168.1.16
      sent      rcvd  rate    rtt     avg    mdev     max     min
         1         1  100       7       7       0       7       7
         2         2  100       4       7       1       7       4
         3         3  100       4       7       2       7       4
VES-1124>
```

Figure 24-9 IP PING Command Example

24.4.2 ip route status

Syntax:

```
ip route status
```

This command displays the routing table. An example is shown next.

```
VES-1124> ip route status
Dest            FF Len Device     Gateway         Metric stat Timer  Use
192.168.1.0     00 24  swp00      192.168.1.1       1    041b 0      17439
172.16.0.0      00 16  swp00      192.168.1.2       2    801b 0      0
127.0.0.0       00 8   swp00      127.0.0.1         1    041b 0      0
VES-1124>
```

Figure 24-10 ip route status Command Example

24.4.3 ip arp status

Syntax:

`ip arp status`

This command displays all interfaces' IP Address Resolution Protocol (ARP) status. An example is shown next.

```
VES-1124> ip arp status
received 2 badtype 0 bogus addr 0 reqst in 0 replies 2 reqst out 1 bad VID 0
cache hit 7 (70%), cache miss 3 (30%)
IP-addr         Type           Time  Addr              stat iface channel
192.168.1.16    Ethernet       250   00:a0:c5:3a:5d:6e 41   swif0 swp24
192.168.1.255   Ethernet       0     ff:ff:ff:ff:ff:ff 43   NULL  NULL
num of arp entries= 2
VES-1124>
```

Figure 24-11 ip arp status Command Example

24.4.4 ip dhcp Commands

Syntax:

`ip dhcp swif0 mode none` (This command disables DHCP on the switch interface (swif0))

`ip dhcp swif0 status` (This command displays the DHCP status on the switch interface (swif0))

An example is shown next.

```
test_mem> ip dhcp swif0 mode none
test_mem> ip dhcp swif0 status
DHCP on iface swif0 is none
```

Figure 24-12 ip dhcp Command Examples

24.5vdsl Commands

These are the commonly used commands that belong to the `vdsl` group of commands. Use "config save" to save these configurations.

24.5.1 vdsl profile list Command

Syntax:

```
vdsl profile list
```

This command displays all VDSL profiles. An example is shown next.

```
VES-1124> vdsl profile list
Profile Name                  | UpSpeed | DownSpeed | UpData | DownData | Auto
------------------------------+---------+-----------+--------+----------+-----
10                            :   18750       16670      187        166     On
11                            :   18750       16670      187        166    Off
12                            :   12500       12500      125        125    Off
13                            :    9380        8330       93         83    Off
14                            :    6250        6250       62         62    Off
15                            :    1560        4170       15         41    Off
20                            :    6250       16670       62        166     On
21                            :    6250        8330       62         83    Off
22                            :    3125        6250       31         62    Off
23                            :    1560        4170       15         41    Off
30                            :    6250       12500       62        125     On
31                            :    6250        9380       62         93    Off
32                            :    3125        6250       31         62    Off
33                            :    1560        4170       15         41    Off
DEFVAL                        :   12500       12500      125        125    Off
VES-1124>
```

Figure 24-13 vdsl profile list Command Example

24.5.2 vdsl profile apply Command

Syntax:

```
vdsl profile apply <profile name> [* | vdsl01 vdsl02 vdsl03 ...vdsl24]
```

This command applies a VDSL profile to the VDSL port(s). The following example applies the Default VDSL profile to all VDSL ports (*).

```
VES-1124> vdsl profile apply Default *
```

Figure 24-14 vdsl profile apply Command Example

24.5.3 vdsl portdetails display Command

Syntax:

```
vdsl portdetail [ * | <chan_s>] [<chan_e>]
```

This command displays the VDSL port details on all or specific VDSL port(s). The following example displays port details from VDSL port 11 to 13.

```
VES-1124> vdsl portdetail vdsl11 vdsl13
< vdsl11 >
Upstream Status:
  Constellation =  QAM 4/Int 32, Rate =  1562500 bps, Fc = 4467773 Hz
  SNR =  0.00dB MSE =  0.00dB PSD =   0.00dBm/Hz RSERR = 0       DISC = 0
Downstream Status:
  Constellation =  QAM 16/Int 24, Rate =  4166666 bps, Fc = 1831054 Hz
  SNR =  0.00dB MSE =  0.00dB PSD = -63.34dBm/Hz RSERR = 0
< vdsl12 >
Upstream Status:
  Constellation =  QAM 4/Int 32, Rate =  1562500 bps, Fc = 4467773 Hz
  SNR =  0.00dB MSE =  0.00dB PSD =   0.00dBm/Hz RSERR = 0       DISC = 0
Downstream Status:
  Constellation =  QAM 16/Int 24, Rate =  4166666 bps, Fc = 1831054 Hz
  SNR =  0.00dB MSE =  0.00dB PSD = -63.34dBm/Hz RSERR = 0
< vdsl13 >
Upstream Status:
  Constellation =  QAM 4/Int 32, Rate =  1562500 bps, Fc = 4467773 Hz
  SNR =  0.00dB MSE =  0.00dB PSD =   0.00dBm/Hz RSERR = 0       DISC = 0
Downstream Status:
  Constellation =  QAM 16/Int 24, Rate =  4166666 bps, Fc = 1831054 Hz
  SNR =  0.00dB MSE =  0.00dB PSD = -63.34dBm/Hz RSERR = 0
VES-1124>
```

Figure 24-15 vdsl port status display Command Example

24.5.4 vdsl setmode Command

Syntax:

```
vdsl setmode [ 0:10BaseS | 1:ANSI | 2:ETSI ]
```

This command sets the VDSL mode on the VES. The following example sets VDSL mode of the VES to 10BaseS.

```
VES-1124> vdsl setmode 0
 set VDSL mode: 10BaseS
All ports are disabled after VDSL mode changed.
VES-1124>
```

Figure 24-16 vdsl setmode Command Example

24.6 Enabling rstp on a VDSL Port

1. First enable RSTP

   ```
   sys sw rstp bridge enable
   ```

2. Then enable RSTP on a VDSL port 1

   ```
   sys sw rstp port enable 1
   ```

3. Save the configuration

   ```
   config save
   ```

Chapter 25
IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands. Use the "config save" command to save configuration changes.

25.1 IEEE 802.1Q Tagged VLAN Overview

See the *VLAN* chapter for more information on VLANs. There are two kinds of tagging:

1. Explicit Tagging

A VLAN identifier is added to the frame header that identifies the source VLAN.

2. Implicit Tagging

The MAC (Media Access Control) number, the port or other information is used to identify the source of a VLAN frame.

The IEEE 802.1Q Tagged VLAN uses both explicit and implicit tagging.

It is important for the switch to determine what devices are VLAN-aware and VLAN-unaware so that it can decide whether to forward a tagged frame (to a VLAN-aware device) or first strip the tag from a frame and then forward it (to a VLAN-unaware device).

25.2 Filtering Databases

A filtering database stores and organizes VLAN registration information useful for switching frames to and from a switch. A filtering database consists of a static entries (Static VLAN or SVLAN table) and dynamic entries (Dynamic VLAN or DVLAN table).

25.2.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

25.2.2 Dynamic Entries (DVLAN Table)

Dynamic entries are learned by the switch and cannot be created or updated by administrators. The switch learns this information by observing what port, source address and VLAN ID (or VID) is associated with a frame. Entries are added and deleted using GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol.

25.3 Configuring Tagged VLAN

The following procedure shows you how to configure tagged VLAN.

1. Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the switch.

- Use the `sys sw vlan1q svlan setentry` command to configure a VLAN ID for each port on the switch.
- Use the `sys sw vlan1q svlan active` command when you are finished configuring the VLAN (see the last step).
- Use the `sys sw vlan1q port defaultVID command` to set the VLAN ID you created for a port to that specific port in the PVID table.
- Use the `sys sw vlan1q svlan active` command to activate the VLAN IDs.

Example:

```
VES-1124> sys sw vlan1q svlan setentry upl 2000 24 fixed tag
for newly create VLAN, please use svlan active <VID> to activate this entry

VES-1124> sys sw vlan1q port defaultVID 24 2000

VES-1124> sys sw vlan1q svlan setentry upl 2001 25 fixed untag
for newly create VLAN, please use svlan active <VID> to activate this entry

VES-1124> sys sw vlan1q port defaultVID 25 2001

VES-1124> sys sw vlan1q svlan active 2000

VES-1124> sys sw vlan1q svlan active 2001
```

Figure 25-1 Tagged VLAN Configuration and Activation Example

2. Configure your management VLAN.

- Use the `sys sw vlan1q svlan setentry` command to configure a VLAN ID (VID 3 in this example) for managing the switch (the "management" or "CPU" VLAN).
- Use the `sys sw vlan1q svlan active` command to activate the new management VLAN ID.

Example:

```
VES-1124> sys sw vlan1q svlan setentry example 3 24 fixed tag
for newly create VLAN, please use svlan active <VID> to activate this entry
VES-1124> sys sw vlan1q svlan active 3
```

Figure 25-2 CPU VLAN Configuration and Activation Example

3. Perform the procedure below to complete the VLAN setup.

    a. Telnet to the operational IP address of the switch.

    b. Use the `sys sw vlan1q svlan cpu` command to set VID 3 as the management VLAN.

    c. Use the `sys sw svlan delentry` command to remove the default VLAN ID (1).

Example:

```
VES-1124> sys sw vlan1q svlan cpu 3

VES-1124> sys sw vlan1q svlan delentry 1
```

Figure 25-3 Deleting Default VLAN Example

25.4 IEEE VLAN1Q Tagged VLAN Configuration Commands

These `sw` (switch) commands allow you to configure and monitor the IEEE 802.1Q Tagged VLAN.

25.4.1 garp status

Syntax:

```
sys sw garp status
```

This command shows the switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

```
VES-1124> sys sw garp status
GARP Timer Status :
        Join Timer = 200 msec
        Leave Timer = 600 msec
        Leave All Timer = 10000 msec
VES-1124>
```

Figure 25-4 GARP STATUS Command Example

25.4.2 garp timer

Syntax:

```
sys sw garp timer timer <join timer(ms)> <leave timer(ms)> <leave all
timer<ms>
```

where

`<join timer (ms)>`	=	This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds.
`<leave timer(ms)>`	=	This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.
`<leave all timer<ms>`	=	This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds.

This command sets the switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
VES-1124> sys sw garp timer 300 800 11000
```

Figure 25-5 garp timer Command Example

25.4.3 gvrp status

Syntax:

```
sys sw gvrp status
```

This command shows the switch's GVRP settings.

An example is shown next.

```
VES-1124> sys sw gvrp status
GVRP control block status:
  gvrpEnable = 0
  gvrpPortEnable:
    XXXXXXXXXXXXXXXXXXXXXXXXXX
VES-1124>
```

Figure 25-6 garp status Command Example

25.4.4 gvrp enable

Syntax:

```
sys sw gvrp enable
```

This command turns on GVRP in order to propagate VLAN information beyond the switch.

25.4.5 gvrp disable

Syntax:

```
sys sw gvrp disable
```

This command turns off GVRP so that the switch does not propagate VLAN information to other switches.

25.4.6 vlan1q port status

Syntax:

```
sys sw vlan1q port status <port>
```

This command shows information about the specified port's VLAN settings.

The following example shows the settings for port 1.

```
VES-1124> sys sw vlan1q port status
Usage: sw vlan1q port status <port>
VES-1124> sys sw vlan1q port status 1
Port 1 VLAN Setup :
Default VLAN ID = 1
VLAN Acceptable Type = All
GVRP = Disable
VES-1124>
```

Figure 25-7 vlan1q port status Command Example

25.4.7 vlan1q port default vid

Syntax:

```
sys sw vlan1q port defaultVID <port> <VID>
```

where

<port>	=	A port number
<VID>	=	The VLAN ID. Valid parameter range = [1 – 4094].

This command sets a default VLAN ID for all untagged packets that come in through the specified port.

The following example sets the default VID of port 1 to 2000.

```
VES-1124> sys sw vlan1q port defaultVID 1 2000
```

Figure 25-8 vlan1q port default vid Command Example

25.4.8 vlan1q port accept

Syntax:

```
sys sw vlan1q port accept <port> <all|tagged>
```

where

<port>	=	A port number
<all|tagged>	=	Specifies all Ethernet frames (tagged and untagged) or only tagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets port 2 to accept only tagged frames.

```
VES-1124> sys sw vlan1q port accept 2 tagged
```

Figure 25-9 vlan1q port accept Command Example

25.4.9 vlan1q port gvrp

Syntax:

```
sys sw vlan1q port gvrp <port> <enable|disable>
```

where

`<port>` = A port number

`<enable|disable>` = Turn GVRP on or off.

This command turns GVRP on or off for the specified port.

The following example turns off GVRP for port 2.

```
VES-1124> sys sw vlan1q port gvrp 2 disable
```

Figure 25-10 vlan1q port gvrp Command Example

25.4.10 vlan1q svlan cpu

Syntax:

```
sys sw vlan1q svlan cpu <VLAN ID>
```

where

`<VID>` = The VLAN ID. Valid parameter range = [1 – 4094].

This command sets the management VLAN (CPU). You can only use ports that are members of this management VLAN in order to manage the switch.

The following example sets VLAN ID 2 to be the CPU (management) VLAN.

```
VES-1124> sys sw vlan1q svlan cpu 2
```

Figure 25-11 vlan1q svlan cpu Command Example

25.4.11 vlan1q svlan setentry

Syntax:

```
sys sw vlan1q svlan setentry <name> <VID> <port> <adctl> <tagctl>
```

where

<name>	=	A name to identify the SVLAN entry.
<VID>	=	The VLAN ID [1 – 4094].
<port>	=	This is the switch port number.
<adctl>	=	This is the registrar administration control flag. Valid parameters = [fixed, forbidden, normal]. Enter fixed to register a <port #> to the static VLAN table with <vid>. Enter normal to confirm registration of the <port #> to the static VLAN table with <vid>. Enter forbidden to block a <port #> from joining the static VLAN table with <vid>.
<tagctl>	=	This is the tag control flag. Valid parameters = [tag|untag]. Enter tag to tag outgoing frames. Enter untag to send outgoing frames without a tag.

This command adds or modifies an entry in the static VLAN table. Display your configuration by using the `sys sw vlan1q svlan list` command. An example of a configuration is shown next.

Modify a Static VLAN Table Example

The following is an example of how to modify a static VLAN table.

```
1.      VES-1124> sys sw vlan1q svlan setentry  2000  1  fixed  tag
2.      VES-1124> sys sw vlan1q svlan setentry  2001  2  fixed  tag
```

Figure 25-12 Modifying the Static VLAN Example

Forwarding Process Example

Tagged Frames

1. First the switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames (see Section 25.4.7).
2. The switch then checks the VID in a frame's tag against the SVLAN table.
3. The switch notes what the SVLAN table says (that is, the SVLAN tells the switch whether or not to forward a frame and if the forwarded frames should have tags).
4. Then the switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

Untagged Frames

1. An untagged frame comes in from the LAN.
2. The switch checks the PVID table and assigns a temporary VID of 1.

3. The switch ignores the port from which the frame came, because the switch does not send a frame to the port from which it came. The switch also does not forward frames to "forbidden" ports.
4. If after looking at the SVLAN, the switch does not have any ports to which it will send the frame, it won't check the port filter.

25.4.12 vlan1q svlan delentry

Syntax:

```
sys sw vlan1q svlan delentry <VID>
```

where

`<VID>` = The VLAN ID [1 – 4094].

This command deletes the specified VLAN ID entry from the static VLAN table

The following example deletes entry 2 in the static VLAN table.

```
VES-1124> sys sw vlan1q svlan delentry 2
```

Figure 25-13 vlan1q svlan delentry Command Example

25.5vlan1q svlan active

Syntax:

```
sys sw vlan1q svlan active <VID>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

25.6vlan1q svlan inactive

Syntax:

```
sys sw vlan1q svlan inactive <VID>
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

25.7vlan1q svlan list

Syntax:

```
sys sw vlan1q svlan list
```

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

For the `AdCtl` section of the last column, "-" is a port set to normal, "x" is a forbidden port and "F" is a fixed port.

For the `TagCtl` section of the last column, "T" is a tagged port, "U" is an untagged port.

```
VES-1124> sys sw vlan1q svlan list
802.1Q VLAN Static Entry:
idx. Name         VID  Active   AdCtl / TagCtl
---- ------------ ---- -------- ------------------------
   0            1    1  active  FFFFFFFFFFFFFFFFFFFFFFFFF
                                 UUUUUUUUUUUUUUUUUUUUUUUUU
VES-1124>
```

Figure 25-14 vlan1q svlan list Command Example

25.7.1 vlan1q status

Syntax:

```
sys sw vlan1q status
```

This command displays the current configuration of the IEEE 802.1Q VLAN.

See the following example shows the default VLAN settings. The default VLAN allows all ports to connect to each other and sets them to send untagged packets.

```
VES-1124> sys sw vlan1q status
802.1Q VLAN Setup :
 GVRP = Disable
 Managament VLAN ID = 1
VES-1124>
```

Figure 25-15 vlan1q status Command Example

Part VII:

Appendices and Index

This part includes the appendices and an index.

Appendix A Troubleshooting

This appendix covers potential problems and possible remedies. After each problem description, some steps are provided to help you to diagnose and to solve the problem.

VDSL LED(s)

A VDSL LED is not on.

Chart 1 Troubleshooting the DSL LED(s)

STEPS	CORRECTIVE ACTION
1	Disconnect the phone wire coming from the **USER** port of the VES and connect the VDSL modem directly to the **USER** port of the VES using a different telephone wire. If the LED turns on, check for a problem with the building's phone wire.
2	Set the VDSL modem to "auto-negotiate". If this is not possible, set it to 100 Mbps, half duplex mode.
3	Use the VDSL CI commands to reset and reconnect the VDSL channel.
4	If the LED remains off, contact the distributor.

Data Transmission

The VDSL LED is on, but data cannot be transmitted.

Table 23-1 Troubleshooting Data Transmission

STEPS	CORRECTIVE ACTION
1	Disconnect the phone wire coming from the USER port of the VES and connect the VDSL modem or router directly to the USER port of the VES using a different telephone wire. If data can be transmitted, check for a problem with the building's phone wire.
2	Check to see that you are using the correct VDSL mode.
3	Check the VLAN configuration of the VES.
4	Do a loopback test on a port from the **Diagnostic** screen.
5	Ping the VES from the user's computer.
6	If you cannot ping, connect the VDSL modem to another VES VDSL port. If the VDSL modem works with a different port, then there may be a problem with the original port. Contact the distributor.
7	If using a different port does not work, try a different VDSL modem or router with the original port.

Intermittent VDSL LED(s)

A VDSL LED turns on and off intermittently.

Table 23-2 Troubleshooting a Non-Constant VDSL LED

STEPS	CORRECTIVE ACTION
1	Disconnect the phone wire coming from the USER port of the VES and connect the VDSL modem or router directly to the USER port of the VES using a different telephone wire. If the VDSL LED stays on, check for a problem with the building's phone wire.
2	Use the VDSL CI commands to reset and reconnect the VDSL channel.

Data Rate

The SYNC-rate is not the same as the configured rate.

Table 23-3 Troubleshooting the SYNC-rate

STEPS	CORRECTIVE ACTION
1	Disconnect the phone wire coming from the USER port of the VES and connect the VDSL modem or router directly to the USER port of the VES using a different telephone wire. If the rates match, the regular phone wire quality may be limiting the speed.
2	Do a local and remote feedback test from menu 24.4 to determine if there are problems with the telephone line.

Configured Settings

The VES's configured settings do not take effect at restart.

Table 23-4 Troubleshooting the VES's Configured Settings

CORRECTIVE ACTION
All VDSL parameters and flags set using VDSL C/I commands are effective at run-time only. If you restart the VES, you will lose the configuration changes you made with CI commands. To save changes permanently, use the appropriate web configurator screen(s). If this does not work, contact the distributor.

Password

I forgot the password to my VES.

Table 23-5 Troubleshooting the Password

STEPS	CORRECTIVE ACTION
1	Upload the default configuration file. All settings will return to the default value and previously saved configurations will be lost.
2	Send a screen shot of your VES's MAC address to your local distributor.

Remote Server

The computer behind the VDSL modem or router cannot access a remote server.

Table 23-6 Troubleshooting a Remote Server

STEPS	CORRECTIVE ACTION
1	See *Table 23-1* to make sure that you are able to transmit to the VES.
2	Make sure the gateway's IP address is the same as the one configured in the user's computer.
3	Check the VLAN configuration of the Ethernet port on the VES.
4	Check the Ethernet cable and connections between the VES and the gateway.
5	Try to access another remote server. If data can be transmitted to a different remote server, the remote server that could not be accessed may have a problem.

Connecting to the Switch

The VES cannot connect to the switch.

Table 23-7 Troubleshooting Connecting to the Switch

STEPS	CORRECTIVE ACTION
1	Check your cable connections. Use a straight through Ethernet cable when connecting the VES to a switch. Use a crossover Ethernet cable if you are daisy-chaining to other switches and make sure trunking is disabled.
2	If Ethernet port trunking is enabled, make sure the switch also supports Ethernet port trunking.
3	The factory default settings for the Ethernet ports of the VES are: Speed: Auto Duplex: Auto Flow control: Enable Trunking: Disabled If the VES's auto-negotiation is turned off, an Ethernet port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the switch Ethernet port are the same in order to connect.

Appendix B
Pin Assignments

These are the Telco-50 cable pin assignments for the VES-1124.

Hardware Telco-50 Connector Pin Assignments

The following diagram shows the pin assignments of the **USER** Telco-50 connectors.

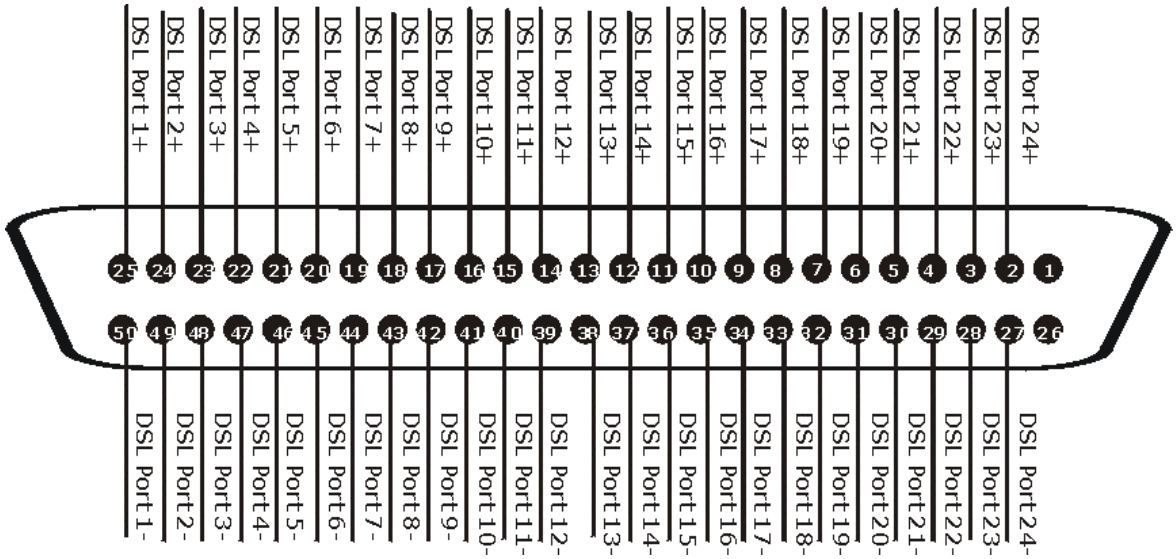


Diagram 1 USER Telco-50 Pin Assignments

The following diagram shows the phone port pin assignments of the **CO** Telco-50 connectors.

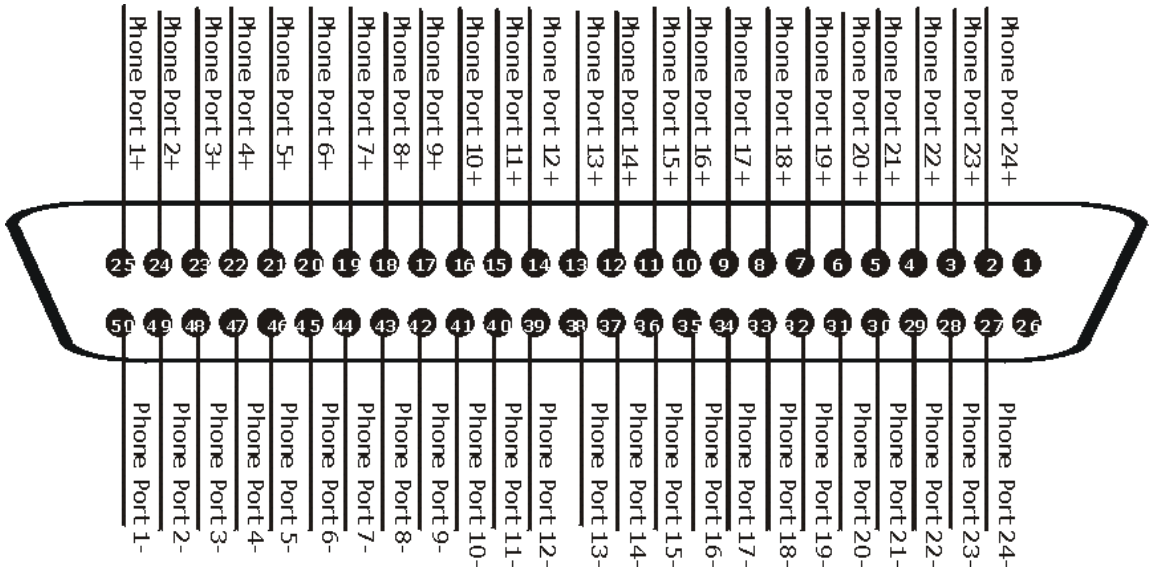


Diagram 2 CO Telco-50 Pin Assignments

This table lists the ports and matching pin numbers for the hardware Telco-50 connectors.

Chart 2Hardware Telco-50 Connector Port and Pin Numbers

PORT NUMBER	PIN NUMBER
1	25, 50
2	24, 49
3	23, 48
4	22, 47
5	21, 46
6	20, 45
7	19, 44
8	18, 43
9	17, 42
10	16, 41
11	15, 40
12	14, 39
13	13, 38
14	12, 37
15	11, 36
16	10, 35
17	9, 34
18	8, 33

Chart 2Hardware Telco-50 Connector Port and Pin Numbers

PORT NUMBER	PIN NUMBER
19	7, 32
20	6, 31
21	5, 30
22	4, 29
23	3, 28
24	2, 27

Appendix C
Product Specifications

These are the VES product specifications.

Chart 3 General Product Specifications

Standards	IEEE802.3 10BASE-T Ethernet (twisted-pair copper) IEEE802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) ANSI/IEEE802.3 Auto-negotiation IEEE802.3x Flow Control IEEE802.1p Priority Queues IEEE802.1Q Tagged VLAN
Interfaces	Front Panel • 10/100BASE-T MDI/MDI-X auto-sensing and auto-negotiating Ethernet Port • Console port • Telco-50 connector
VDSL Upstream Rates Parameters (10BaseS Mode)	1.56Mbps, QAM4, Baud = 25M/32, fc= 4.467773MHz 6.25Mbps, QAM4, Baud = 25M/8, fc= 5.810546MHz 9.38Mbps, QAM8, Baud = 25M/8, fc= 5.810546MHz 12.50Mbps, QAM16, Baud = 25M/8, fc= 5.810546MHz 18.75Mbps, QAM64, Baud = 25M/8, fc= 5.810546MHz
VDSL Downstream Rates Parameters (10BaseS Mode)	4.17Mbps, QAM16, Baud = 25M/24, fc=1.831054MHz 6.25Mbps, QAM8, Baud = 25M/12, fc= 1.953125 MHz 8.33Mbps, QAM16, Baud=25M/12, fc=1.953125MHz 12.50Mbps, QAM64, Baud = 25M/12, fc= 1.953125 MHz 16.67Mbps, QAM256, Baud = 25M/12, fc= 1.953125 MHz
VDSL Upstream Rates Parameters (ANSI Mode)	1.56Mbps, QAM4, Baud = 25M/32, fc= 4.467773MHz 3.13M QAM16, Baud=25M/24, fc=4.46773MHz 6.25Mbps, QAM256, Baud = 25M/32, fc= 4.467773MHz
VDSL Downstream Rates Parameters (ANSI Mode)	4.17Mbps, QAM16, Baud = 25M/24, fc=1.831054MHz 6.25Mbps, QAM8, Baud = 25M/12, fc= 1.953125 MHz 8.33Mbps, QAM16, Baud=25M/12, fc=1.953125MHz 12.50Mbps, QAM64, Baud = 25M/12, fc= 1.953125 MHz 16.67Mbps, QAM256, Baud = 25M/12, fc= 1.953125 MHz
VDSL Upstream Rates Parameters (ETSI Mode)	1.56Mbps, QAM4, Baud = 25M/32, fc= 4.467773MHz 3.13M QAM16, Baud=25M/24, fc=4.46773MHz 6.25Mbps, QAM256, Baud = 25M/32, fc= 4.467773MHz
VDSL Downstream Rates Parameters (ETSI Mode)	4.17Mbps, QAM16, Baud = 25M/24, fc=1.831054MHz 6.25Mbps, QAM8, Baud = 25M/16, fc= 1.831054MHz 9.38Mbps, QAM64, Baud=25M/16, fc=1.831054MHz 12.50Mbps, QAM256, Baud = 25M/16, fc= 1.831054MHz
VDSL Splitter Parameters (3db Frequency range)	10BaseS: Downstream: 900KHz to 3.0MHz Upstream: 4.0MHz to 7.9MHz ETSI Plan 997: Downstream: 900KHz to 2.7Mhz Upstream: 4.0MHz to 5.0MHz ANSI/ ETSI Plan 998: Downstream: 900KHz to 3.0MHz Upstream: 4.0MHz to 5.0MHz

Chart 3 General Product Specifications

Compatible CPE Device Model	Prestige 841 Prestige 841-25

Chart 4 Performance and Management Specifications

VDSL	Fixed Rate and Rate Adaptive. Power Back Off (PBO)
Diagnostics Capabilities	The switch can perform self-diagnostic tests. These tests check the operation of the following circuits: FLASH memory DRAM LAN port local & remote loopback test Per VDSL port loopback test HTP items
VLAN	IEEE 802.1Q tag-based VLAN, 4094 Max
Security	Static MAC address forward Block unresolved address forwarding/Port security 802.1x port authentication
Multicasting	Support IGMP snooping IGMP V1 and V2 (RFC2236 and RFC112)
Bridging	6K MAC addresses (hashed) Static MAC address forwarding, 32 entries Broadcast storm control Automatic address learning and aging Aging time from 10 to 765 seconds in 1 second increment (default 300 seconds)
Switching	8.8Gbps, non-blocking Maximum frame size: 1522 bytes including tag/CRC Store and forward
QoS	802.1p Two priority queues Queuing Algorithm: FCFS/SP/WRR Port-based bandwidth control from 100Kbps to 100Mbps (by 1518bytes packets) IGMP snooping
Port Mirroring	Port-based mirroring to a monitor port
Clustering (iStacking)	Clustering master or slave member Manage up to 24 cluster member devices
Broadcast Storm	Support broadcast storm control
System Management	Configuration via console/telnet/web Firmware upgrade via FTP/web/console Configuration backup and restore via FTP/web/console System management access control Multi-login, single management. System clock: manual setup or NTP SNMP v2c RMON group 1,2,3,9 ICMP echo/echo reply
Management Security	User ID/Password for Telnet and Web-based management authentication Up to five administrators allowed

Chart 4 Performance and Management Specifications

MIBs	RFC1213 RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 RMON RFC1155 SMI RFC2647 Bridge MIB extension (for 802.1Q) VDSL private MIB

Chart 5 Physical and Environmental Specifications

Weight	6 kg
Power Supply	+15V power supply from the back panel.
Fuse Rating	One 5mm (D) x 20mm (L), T type, 3 amp, 250 Volt AC fuse. **Caution: For continued protection against risk of fire, replace only with the same type and fuse rating.**
Temperature Threshold	There are three temperature sensors on the VES-1124: • T1 (VDSL Chipset): 65 °C ON; 60 °C OFF • T2 (Power): 70 °C ON; 65 °C OFF • T3 (Switch): 65 °C ON; 60 °C OFF
Voltage Threshold	There are 6 voltages on the VES-1124: • 1.8V Digital: +- 5% • 1.8V Analog: +- 5% • 2.5V: +- 5% • 3.3V: +- 5% • 5V: +- 5% • 15V: +- 5%
Operating Temperature	0 ~ 50°C
Storage Temperature	-25 ~ 70°C
Operational Humidity	5 ~ 95% (non-condensing)
Certifications	Safety • UL60950-1 • CSA60950-1 • EN60950 –1 • IEC60950-1 • ITU-T K.21 (Version 2000) EMC • CE-ENC Class A • FCC Part 15 Class A

Index

8

802.1Q VLAN Type 5-7

A

Acceptable Frame Type 6-6
Actual Rate 5-13
Aging Time 5-7
Airflow 2-3
All Connected 6-12
authenticationFailure 15-3

B

Backup Configuration 18-3
Band Plan 5-13, 5-14
  10BaseS 5-13
  ANSI/ETSI Plan 998 Mode 5-13
  ETSI Plan 997 5-13
Bridge ID 8-3
Bridge Priority 8-6
Broadcast Storm Control 10-1

C

Canonical Format Indicator 6-1
CE Mark Warning iii
Certifications iii
CFI ..... *See* Canonical Format Indicator
CLI Command ..... 3-7, VII
  Configure tagged VLAN example 25-2
  Getting help 23-2
  Static VLAN Table example 25-7
  sys Commands 23-2
CO port 2-1
CO Telco-50 Connectors ..... A
Cold Start 15-3
Command
  exit command 23-11
  ip commands 23-12
  Summary 23-2
  vdsl commands 23-13
Command
  Command conventions 23-1
  Forwarding Process Example 25-7
  IEEE 802.1Q Tagged VLAN commands example 25-1
  Syntax conventions 23-2
  sys sw Commands 23-6
Command Line Interface ..... 3-7, VII
  Accessing 23-1
  Introduction 23-1
Commands
  config save 23-14
config save 23-1, 23-6, 23-7, 23-15
Configured Settings ..... B
Console Port 2-1
Contact Person's Name 5-5
Contacting Customer Support v
Cost to Bridge 8-3
Curbside Application 1-4

D

Data Rate ..... B
Data Transmission ..... A
Daytime (RFC 867) 5-5
Disclaimer ii
Domain Name Server 5-9
Dropped Packet 4-11
Duplex 5-12
DVLAN Table 25-1

E

egress port 6-13
Ethernet Address 5-3
Ethernet Port Test 19-2
Ethernet port trunking C
exit Command
  summary 23-11

F

FCC iii
FCC Warning iii
File Transfer using FTP 18-4
  command example 18-4
  GUI-based 18-5
  procedure 18-5
  restrictions over WAN 18-6
Filename Conventions 18-4
Filtering Databases 25-1
Firmware Upgrade 18-1
Flow Control 5-12
Forgot the password ..... B
Forwarding Delay 8-3, 8-6
  general rule 8-6
Frequency Band Plans 5-13
Frimware version 5-2
FTP 18-4

G

GARP ..... 25-1. *See* Generic Attribute Registration Protocol
garp status 25-3
GARP Status Command 25-3
GARP Terminology 6-2
garp timer 25-3
GARP Timer 5-8
General Setup 5-1, 5-4
General Syntax Conventions xiv
Generic Attribute Registration Protocol 6-2
Get Community 15-4
GetNext 15-2
Glossary and ZyXEL Web Site xiv
GVRP 6-6, 25-1
GVRP (GARP VLAN Registration Protocol) 6-2, 6-6
gvrp disable 25-4
gvrp enable 25-4
gvrp status 25-4

H

Hardware Monitor
  Fans 5-3
  Temperature unit 5-3
Hello Time 8-3, 8-6
Help 3-8

I

IEEE 802.1p 5-8
IEEE 802.1Q ..... *See* Tagged VLAN
IEEE 802.1Q Tagged VLAN 25-1
IEEE 802.1x 13-1
IGMP Snooping 5-6
Ingress Check 6-6
Ingress filtering 6-2
Interference Statements iii
Intermittent VDSL LED ..... B
IP Address 5-9
ip arp status 24-6
ip Commands
  examples 24-5
  summary 23-11
ip ping 24-5
ip route status 24-5
IP Setup 5-1, 5-9
IP Subnet Mask 5-9
iStacking 20-1

J

Join Timer 5-8

L

LACP
  Timeout 12-4
Leave All Timer 5-8
Leave Timer 5-8
Link aggregation ID 12-4
linkDown 15-3
Location 5-5
Login Accounts 15-4

M

MAC 5-3
MAC address 5-3
MAC address learning 1-3, 5-7, 7-1

MAC Address Learning 5-7
Management Information Base (MIB) 15-2
Management VLAN ID 5-10
Max Age 8-3, 8-6
Media Access Control 5-3
MIBs ..... G
mini POP 1-4
Mirror port 11-1
Mirror Setup 11-3

N

Naming Conventions xiv
Navigation Panel Links 3-4
NTP (RFC-1305) 5-5

O

Online Registration xiv
Operating Temperature ..... G
Operational Humidity ..... G

P

P841 1-4
Password
  Default 3-1
PBO 5-14
PBO (Power Back Off) 5-13
Ping 19-2
Port Based VLAN Type 5-7
Port Details 4-4, 4-5
Port Isolation 6-12
Port Mirroring 11-1, 23-10
Port Setup 5-10, 5-11
Port Statistics ..... *See* Port Details
Port Status ..... 4-2. *See* Port Details
Port VID 6-2
  Default for all ports 6-1
Port-based VLANs 6-10
  Configure 6-10
Power Supply ..... G
Priority 5-8
Priority Level 5-8
Priority Queue Assignment 5-8
Product specifications ..... E
Profile 5-15
PSD (Power Spectral Density) 5-13
PVID 6-6

R

RADIUS (Remote Authentication Dial-In User Service) 13-1
RADIUS Setup 13-2
ras 18-4
Ras 18-4
Rate Adaption 5-13
  Fixed Rate 5-14
  Rate Adaptive Decrease Mode 5-14
Rear Panel Connections
  Rear Panel 2-3
Reauthentication 13-4
Related Documentation xiv
Remote Management 15-6
Remote Server C
repair iv
Resetting the Switch 3-7, 3-8
Restore Configuration 18-2
Revolutions Per Minute (RPM) 5-3
Rom-0 18-4
Runt 4-7
Rx KB/s 4-3, 4-10
Rx Packet 4-10
RxPkts 4-3, 4-10

S

Safety ..... G
Screen Overview 3-5
Secured Client 18-6
Server Port 15-6
Service iv
Service Access Control 15-6
Set Community 15-4
Shared Secret 13-2
Simple Network Management Protocol 15-2
SNMP 15-2
  Configuring 15-3
    Trap 15-4

Get 15-2
Manager 15-2
MIBs 15-3
supported versions 15-2
Trap 15-3
SNMP Commands 15-2
SNMP Traps 15-3
Splitter Chassis Rear Panel Telco-50 Pin Assignments ..... A
standard browser 3-1
Standards ..... E
Static MAC Forwarding 7-1
Static Route
Setup 17-1
Summary table 17-2
Static VLAN 6-6
Control 6-8
Summary Table 6-8
Tagging 6-8
Status 4-2
STP Path Costs 8-1
STP Port States 8-2
SVLAN Table 25-1
Switch Lockout 3-6
Switch Setup 5-6, 6-3
Synchronized Ports 12-3
SYNC-rate ..... B
sys Commands
examples 24-1
Summary 23-2
sys ixe2424 pktcnt 24-2
sys log clear 24-1
sys log disp 24-1
sys sw commands
summary 23-6
sys sw mac list 24-3
sys sw vlan1q vlan list 24-2
sys version 24-1
System Information 5-1
System Log 19-1
System Name 5-4
System Priority 12-4
System up Time 4-3

T

Tag Control Information 6-1
Tag Protocol Identifier 6-1
Tagged VLAN 6-1
GARP 6-2
GVRP 6-2
Memebership Registration 6-1
Taiwanese BSMI A Warning iii
TCI ..... *See* Tag Control Information
Terminal emulation 2-1
Terminal Emulation 2-1, 23-1
Time (RFC-868) 5-5
Time server protocol supported 5-5
TPID ..... *See* Tag Protocol Identifier
Trademarks ii
Trap 15-4
trusted computers 15-7
TX Collision 4-11
Tx KB/s 4-3, 4-10
Tx Packet 4-10
TxPkts 4-3, 4-10

U

Up Time 4-3
USER port 2-1
USER Telco-50 Connectors ..... A
Username
Default 3-1

V

VDSL Parameters 5-13
VDSL Profile 5-14
VID ..... 6-4. *See* VLAN Identifier
VLAN
Explicit Tagging 25-1
Forwarding 6-1
ID (VID) 25-1
Implicit Tagging 25-1
Introduction 5-5
Port-based 6-10
Priority frame 6-1
Registration Information 25-1

VLAN Administrative Control 6-2
VLAN Group 6-8
VLAN ID 5-10, 6-1
  maximum number of 6-1
VLAN Identifier 6-1
VLAN Port Settings 6-4
VLAN Status 6-3
VLAN Tag Control 6-2
VLAN Type 5-7, 6-3
vlan1q port accept 25-5
vlan1q port default vid 25-5
vlan1q port gvrp 25-6
vlan1q port status 25-5
vlan1q svlan active 25-8
vlan1q svlan cpu 25-6
vlan1q svlan delentry 25-8
vlan1q svlan inactive 25-8
vlan1q svlan list 25-8
vlan1q svlan setentry 25-6
VT100 ..... 2-1, 23-1

W

WarmStart 15-3
Web Configurator
  Logging out 3-8
  Online help 3-8
  Recommended browsers 3-1

X

XMODEM upload 3-8

Z

ZyNOS (ZyXEL Network Operating System) 18-4
ZyNOS Firmware version 5-2
ZyXEL Limited Warranty
  Note iv